



Cisco Unified SCCP および SIP SRST システム管理者ガイド (全バージョン用)

2018 年 3 月 30 日

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
所在地、電話番号、FAX 番号
は以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices

**【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/) 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。
リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、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と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。製品の使用にあたってのすべての責任は、ユーザ側にあります。

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。このソフトウェアライセンスまたは限定保証を見つけられない場合は、CISCO の代理店に連絡しコピーを入手してください。

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco Unified SCCP および SIP SRST システム管理者ガイド(全バージョン)
© 2018 Cisco Systems, Inc. All rights reserved.



はじめに	i
対象読者	ii-i
表記法	ii-i
マニュアルの入手方法およびテクニカル サポート	ii-ii
Cisco Unified Survivable Remote Site Telephony 機能のロードマップ	iii-iii
目次	iii-iii
マニュアルの構成	iii-iv
機能のロードマップ	iii-v
Cisco Unified SRST の新機能について	iii-xi
Unified SRST バージョン 12.1 の新機能	iii-xi
Unified SRST バージョン 12.0 の新機能	iii-xi
Cisco Unified SRST バージョン 11.0 の新機能	iii-xii
Cisco Unified SRST バージョン 10.5 の新機能	iii-xii
Cisco Unified DX650 SIP IP Phone のサポート	iii-xii
Cisco Unified 78xx SIP IP Phone のサポート	iii-xii
Cisco Unified SRST バージョン 10.0 の新機能	iii-xii
Cisco Jabber for Windows	iii-xiii
Cisco Unified SIP IP Phone のバージョン ネゴシエーション	iii-xiii
Cisco Unified SRST バージョン 9.5 の新機能	iii-xiii
after-hours パターン ブロッキングでの正規表現のサポート	iii-xiv
コール パークの再コールの機能拡張	iii-xv
パーク モニタリング	iii-xv
コールされたボイス ハント グループの名前の表示のサポート	iii-xvi
ボイス ハント グループの最終エージェントへのローカル コール転送の防止	iii-xvii
Cisco Unified SIP IP Phone における、電話料金詐欺行為防止を目的としたトランク間転送ブロッキング	iii-xvii
conference-pattern blocked	iii-xx
電話会議に対する最大桁数の設定	iii-xx
前提条件	iii-xx
手順の詳細	iii-xxi
電話機で電話会議ブロッキング オプションを設定する	iii-xxii
前提条件	iii-xxii

transfer-pattern blocked	iii-xxiii	
Cisco Unified SRST バージョン 9.1 の新機能	iii-xxiv	
Cisco Unified SIP IP Phone の KEM のサポート	iii-xxv	
スピードダイヤルサポートの機能強化	iii-xxv	
ボイスハントグループのサポート	iii-xxvi	
Cisco Unified SRST バージョン 9.0 の新機能	iii-xxvi	
Cisco Unified 6901 および 6911 SIP IP Phone のサポート	iii-xxvii	
Cisco Unified 6921、6941、6945、および 6961 SIP IP Phone のサポート	iii-xxvii	iii-xxvii
Cisco Unified 8941 および 8945 SIP IP Phone のサポート	iii-xxvii	
回線ごとの複数コール	iii-xxvii	
Cisco ATA-187 での音声とファクスのサポート	iii-xxviii	
Cisco Unified SRST バージョン 8.8 の新機能	iii-xxviii	
Cisco Unified 6945、8941、および 8945 SCCP IP Phone のサポート	iii-xxviii	iii-xxviii
Cisco Unified SRST バージョン 8.0 の新機能	iii-xxviii	
Cisco Unified SRST バージョン 7.0/4.3 の新機能	iii-xxix	
Cisco Unified SRST バージョン 4.2(1) の新機能	iii-xxix	
Cisco Unified SRST バージョン 4.1 の新機能	iii-xxix	
Cisco Unified SRST バージョン 4.0 の新機能	iii-xxix	
Cisco Unified IP Phone の追加サポート	iii-xxix	
Cisco IP Communicator のサポート	iii-xxx	
SCCP および ATA サポートを使用した FAX パススルー	iii-xxx	
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 (SCCP 電話)	iii-xxx	
ビデオサポート	iii-xxx	
Cisco Unified SRST バージョン 3.4 の新機能	iii-xxx	
Cisco SIP SRST 3.4	iii-xxx	
Cisco SRST バージョン 3.3 の新機能	iii-xxx	
セキュア SRST	iii-xxx	
Cisco Unified IP Phone 7970G および Cisco Unified 7971G-GE のサポート	iii-xxx	
show ephone コマンドの機能拡張	iii-xxx	
Cisco SRST バージョン 3.2 の新機能	iii-xxx	
alias コマンドの機能拡張	iii-xxx	
cor コマンドの機能拡張	iii-xxx	
pickup コマンドの機能拡張	iii-xxx	
user-locale コマンドの機能拡張	iii-xxx	
Cisco 3845 でサポートされる Cisco Unified IP Phone の台数増加	iii-xxx	iii-xxx
MOH ライブフィードのサポート	iii-xxx	
コールプリザベーションのタイムアウトなし	iii-xxx	

RFC 2833 DTMF リレーのサポート	iii-xxxiv	
トランスレーションプロファイルのサポート	iii-xxxiv	
Cisco SRST バージョン 3.1 の新機能	iii-xxxv	
Cisco Unified IP Phone 7920 のサポート	iii-xxxv	
Cisco Unified IP Phone 7936 のサポート	iii-xxxv	
Cisco SRST バージョン 3.0 の新機能	iii-xxxv	
IP Phone のディスプレイに対する追加の言語オプション	iii-xxxvi	
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 (SCCP 電話)	iii-xxxvi	
Cisco Unified IP Phone 用にカスタマイズされたシステム メッセージ	iii-xxxvi	iii-xxxvi
二重回線モード	iii-xxxvii	
E1 R2 シグナリングのサポート	iii-xxxvii	
欧州の日付形式	iii-xxxviii	
二重回線モードのハントストップ	iii-xxxviii	
フラッシュ ファイルからのマルチキャスト用の保留音	iii-xxxviii	iii-xxxviii
呼び出しタイムアウトのデフォルト	iii-xxxix	
2 次ダイヤルトーン	iii-xxxix	
show ephone コマンドの機能拡張	iii-xxxix	
電話機の登録に関するシステム ログ メッセージ	iii-xxxix	
3 者間の G.711 アドホック会議	iii-xxxix	
Cisco VG248 Analog Phone Gateway 1.2(1) 以降のバージョンのサポート	iii-xxxix	
Cisco SRST バージョン 2.1 の新機能	iii-xl	
IP Phone のディスプレイに対する追加の言語オプション	iii-xl	iii-xl
Cisco SRST の集約	iii-xli	
Cisco ATA 186 および ATA 188 のサポート	iii-xli	
Cisco Unified IP Phone 7902G のサポート	iii-xli	
Cisco Unified IP Phone 7905G のサポート	iii-xli	
Cisco Unified IP Phone 7912G のサポート	iii-xli	
Cisco Unified IP Phone 7914 拡張モジュールのサポート	iii-xlii	iii-xlii
dialplan-pattern コマンドの機能拡張	iii-xlii	
Cisco SRST バージョン 2.02 の新機能	iii-xlii	
Cisco Unified IP Phone Conference Station 7935 のサポート	iii-xlii	iii-xlii
電話番号の増加	iii-xliii	
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	iii-xliii	
次の作業	iii-xliii	
Cisco Unified SRST 機能の概要	1-1	
目次	1-1	

Cisco Unified SCCP SRST	1-1
SCCP SRST について	1-2
Cisco Unified SCCP SRST を設定するための前提条件	1-4
Cisco Unified Communications Manager のインストール	1-5
Cisco Unified SCCP SRST のインストール	1-5
Cisco Unified SCCP SRST と Cisco Unified Communications Manager の統合	1-5
Cisco Unified SCCP SRST の設定に関する制約事項	1-7
Cisco Unified SIP SRST	1-9
SIP SRST について	1-9
Cisco Unified SIP SRST を設定するための前提条件	1-9
Cisco Unified SIP SRST の設定に関する制約事項	1-10
Cisco Unified SRST のライセンス	1-13
Cisco Unified SRST の無期限ライセンス	1-13
Collaborative Professional Suite ライセンス	1-13
Cisco Smart License	1-14
Call Home の設定	1-16
ライセンス モード	1-17
制限事項	1-18
Unified CME と Unified SRST のインターフェイス サポート	1-18
MGCP ゲートウェイと SRST	1-18
Unified SRST SIP IP Phone の IPv6 サポート	1-19
Unified SRST SIP IP Phone での IPv6 の機能サポート	1-19
制限事項	1-19
SIP IP Phone の IPv6 プールの設定	1-20
SIP IP Phone の IPv6 プールの設定例	1-24
Cisco Unified IP Phone およびプラットフォームのサポート	1-25
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	1-25
Cisco Unified IP Phone のサポート	1-25
プラットフォームとメモリのサポート	1-26
Cisco Feature Navigator を使用したプラットフォーム サポートの確認	1-26
Cisco IOS ソフトウェア イメージの可用性	1-26
Cisco Unified Communications Manager の互換性	1-26
信号のサポート	1-26
言語のサポート	1-26
スイッチのサポート	1-27
次の作業	1-27
その他の関連資料	1-28
関連資料	1-28
標準	1-29

MIB	1-30
RFC	1-30
テクニカル サポート	1-30
マニュアルの入手方法およびテクニカル サポート	1-30
Cisco Unified Enhanced Survivable Remote Site Telephony	2-31
目次	2-31
Unified E-SRST の概要	2-31
Unified-ESRST の利点	2-32
ボイス ハント グループのサポートがある Unified E-SRST	2-32
Unified E-SRST での B-ACD のサポート	2-33
Unified E-SRST でのボイス ハント グループ設定の推奨事項	2-34
Unified E-SRST リリース 12.2 の制限事項	2-34
SIP: Unified E-SRST の設定	2-35
制約事項	2-36
E-SRST モードの有効化	2-36
SIP 共有回線の設定	2-37
BLF の設定	2-37
電話番号の表示の有効化	2-37
音声レジスタ プールのBLFの有効化:	2-38
CUCM のダイジェスト クレデンシャルの設定	2-39
Unified E-SRST でのボイス ハント グループの設定	2-40
手順の詳細	2-41
ボイス ハント グループが強化された Unified E- SRST の設定例	2-45
Unified E-SRST での B-ACD の設定例	2-46
Unified E-SRST でのボイス ハント グループとの共有回線の設定例	2-47
SCCP: Unified E-SRST の設定	2-50
前提条件	2-50
Unified E-SRST のスケール サポート	2-51
次の作業	2-52
ネットワークの設定	3-53
目次	3-53
ネットワークの設定に関する情報	3-53
ネットワークの設定方法	3-54
IP ルーティングのイネーブル化	3-54
MGCP ゲートウェイでの Cisco Unified SRST のイネーブル化	3-54
Cisco IOS リリース 12.3(14)T よりも前の MGCP ゲートウェイでの Cisco Unified SRST の設定	3-54

Cisco IOS リリース 12.3(14)T 以降のリリースを使用した MGCP ゲートウェイでの Cisco Unified SRST の設定	3-56
制約事項	3-56
Cisco IOS リリース 12.3(14) T を使用した MGCP ゲートウェイで SRST をイネーブルにする設定例	3-57
Cisco Unified SRST Phone での DHCP の設定	3-59
単一の DHCP IP アドレス プールの定義	3-59
Cisco Unified IP Phone ごとの個別の DHCP IP アドレス プールの定義	3-60
DHCP リレー サーバの定義	3-61
キープアライブ インターバルの指定	3-62
例	3-63
次の作業	3-63
Cisco Unified SIP SRST 4.1	4-65
目次	4-65
Cisco Unified SIP SRST 4.1 の前提条件	4-65
Cisco Unified SIP SRST 4.1 の制約事項	4-66
Cisco Unified SIP SRST 4.1 に関する情報	4-66
Out-Of-Dialog REFER	4-66
SIP 電話の桁収集	4-67
KPML 桁収集	4-67
SIP ダイアルプラン	4-67
発信者 ID 表示	4-68
コール自動転送およびコール転送の SIP 補足サービスのディセーブル化	4-68
アイドルプロンプト ステータス	4-68
Enhanced 911 サービス	4-69
Cisco Unified SIP SRST 4.1 機能の設定方法	4-69
SIP 電話の KPML の有効化	4-69
制約事項	4-69
次の作業	4-70
コール自動転送およびコール転送の SIP 補足サービスのディセーブル化	4-71
SIP 電話のアイドルプロンプト ステータスの設定	4-72
前提条件	4-72
次の作業	4-73
SCCP を用いた Cisco Unified IP Phone の設定	5-75
目次	5-75
Cisco Unified IP Phone の設定に関する情報	5-75
Cisco Unified IP Phone の設定方法	5-76
電話機能をサポートするための Cisco Unified SRST の設定	5-76

Cisco Unified 8941 および 8945 SCCP IP Phone の設定	5-78
Cisco Unified SRST がイネーブルであることの確認	5-79
IP Phone の時計、日付、時刻形式の設定	5-80
例	5-81
IP Phone の言語表示の設定	5-82
例	5-83
Cisco Unified IP Phone 用にカスタマイズしたシステム メッセージの設定	5-83
例	5-84
2 次ダイヤル トーンの設定	5-84
例	5-85
二重回線の電話設定	5-85
例	5-86
各ボタンで 8 つのコールの設定(オクトライン)	5-87
前提条件	5-87
制約事項	5-87
例	5-89
コールの最大数の設定	5-89
前提条件	5-89
トラブルシューティング	5-90
Cisco Unified SRST 向けの Cisco IP Communicator の設定方法	5-91
前提条件	5-91
Cisco IP Communicator の確認	5-92
Cisco IP Communicator のトラブルシューティング	5-92
次の作業	5-92
SIP を用いた Cisco Unified IP Phone の設定	6-93
目次	6-93
SIP レジストラを設定するための前提条件	6-93
SIP レジストラの設定に関する制約事項	6-93
SIP レジストラの設定に関する情報	6-93
SIP レジストラの設定方法	6-94
SIP レジストラの設定	6-94
次の作業	6-96
SIP 電話へのバックアップ レジストラ サービスの設定	6-96
前提条件	6-96
制約事項	6-96
次の作業	6-99
SIP 電話へのバックアップ レジストラ サービスの設定(オプション コマンドを使用)	6-99
前提条件	6-99
例	6-102

SIP レジストラ設定の確認	6-103
プロキシダイアルピア設定の確認	6-104
次の作業	6-107
コール処理の設定	7-109
目次	7-109
バックツーバック ユーザ エージェント モードを使用する SIP SRST 機能を設定するための前提条件	7-109
バックツーバック ユーザ エージェント モードを使用する SIP SRST 機能の設定における制約事項	7-110
SCCP SRST コール処理の設定について	7-110
WAN リンク障害用の H.323 VoIP コールプリザベーション拡張機能	7-110
電話料金詐欺行為防止	7-110
バックツーバック ユーザ エージェント モードを使用する SIP SRST 機能の設定について	7-111
Cisco Unified SIP SRST および Cisco SIP Communications Manager Express の共通機能	7-111
Cisco Unified SCCP SRST の設定方法	7-113
着信コールの設定	7-114
話中信号または無応答時のコール転送の設定	7-114
例	7-115
コール再ルーティングの設定	7-115
例	7-118
コール ピックアップの設定	7-118
例	7-120
コンサルタティブ転送の設定	7-120
会議コール	7-121
転送の桁収集方法の設定	7-122
例	7-123
グローバルプレフィックスの設定	7-123
例	7-124
桁トランスレーションルールの有効化	7-125
例	7-126
トランスレーションプロファイルの有効化	7-126
例	7-129
トランスレーションプロファイルの確認	7-129
ダイヤルピア チャンネルハントの設定	7-130
例	7-130
話中タイムアウトの設定	7-131
例	7-131

呼び出しタイムアウトのデフォルトの設定	7-131
例	7-132
発信コールの設定	7-132
ローカルおよびリモート コール転送の設定	7-133
例	7-133
Cisco SRST 3.0 で H.450.2 および H.450.3 を使用したコンサルタティブ コールの転送および自動転送の有効化	7-133
例	7-136
Cisco SRST 3.0 以前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	7-137
例	7-141
トランク アクセスコードの設定	7-141
例	7-142
桁間タイムアウト値の設定	7-142
例	7-143
制限クラスの設定	7-143
例	7-145
時刻、曜日、または日付に基づくコールブロッキング(ツールバー)	7-147
例	7-148
Cisco Unified SIP SRST の設定方法	7-149
SIP 電話の機能の設定	7-149
SIP 間のコール転送の設定	7-151
時刻、曜日、または日付に基づくコールブロッキングの設定	7-153
例	7-156
検証	7-156
SIP のコール保留と保留解除	7-156
例	7-156
オプション機能の設定方法	7-158
3 者間 G.711 アドホック会議の有効化	7-159
例	7-159
XML API スキーマの定義	7-160
コール処理の設定例	7-160
例: キー拡張モジュールのステータスのモニタリング	7-160
例: Cisco Unified SIP SRST での音声ハント グループの設定	7-161
次の作業	7-161
SCCP および SIP のセキュア SRST の設定	8-163
目次	8-163
セキュア SRST を設定するための前提条件	8-163
セキュア SRST の設定に関する制約事項	8-164

セキュア SRST の設定について	8-165	
セキュア SRST の利点	8-165	
Cisco 4000 シリーズ サービス統合型ルータでのセキュア SRST サポート		8-166
セキュア保留音	8-166	
非セキュア SRST での Cisco IP Phone のクリアテキスト フォールバック		8-167
Unified SRST でのシグナリングのセキュリティ (TLS)	8-167	
SRST ルータおよび TLS プロトコル	8-167	
セキュア SRST での証明書の操作	8-167	
CUCM からセキュア SRST への証明書の転送	8-169	
Unified SRST でのメディアのセキュリティ (SRTP)	8-169	
Cisco Unified IP Phone へのセキュアな Cisco Unified SRST の確立		8-170
セキュア SRST の認証および暗号化	8-172	
セキュアな Unified SRST の設定方法	8-173	
セキュア通信のための Cisco Unified SRST ルータの準備	8-174	
Cisco IOS 証明書サーバでの認証局サーバの設定	8-174	
CA サーバに対するセキュアな Cisco Unified SRST ルータの自動登録と認証	8-176	
自動証明書登録の無効化	8-178	
次の作業	8-179	
証明書登録の確認	8-179	
セキュアな Cisco Unified SRST ルータでのクレデンシャル サービスの有効化	8-181	
クレデンシャル設定のトラブルシューティング	8-182	
セキュアな 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	8-183	
Cisco Unified Communications Manager 4.X.X 以前のバージョン		8-183
Cisco Unified Communications Manager 5.0 以降のバージョン		8-184
Cisco Unified Communications Manager 6.0 以降のバージョン		8-185
Cisco Unified SRST ルータでのインポートされた証明書の認証		8-185
次の作業	8-186	
例	8-186	
セキュアな Cisco Unified SRST ルータへの Cisco Unified Communications Manager の設定	8-191	
Cisco Unified Communications Manager への SRST リファレンスの追加		8-191
Cisco Unified Communications Manager での SRST フォールバックの設定	8-192	
Cisco Unified Communications Manager での CAPF の設定	8-193	
セキュアな Cisco Unified SRST ルータでの SRST モードの有効化		8-194
例	8-195	
セキュア SCCP SRST の設定	8-195	
セキュア SCCP SRST を設定するための前提条件	8-195	

セキュア SCCP SRST の設定に関する制約事項	8-196
電話機のステータスおよび登録の確認	8-196
セキュア SCCP SRST の設定例	8-203
Cisco SRST でのセキュアな SIP コール シグナリングおよび SRTP メディアの設定	8-209
Cisco SRST でセキュアな SIP コール シグナリングおよび SRTP メディアを設定するための前提条件	8-209
Cisco SRST でのセキュアな SIP コール シグナリングおよび SRTP メディアの設定に関する制約事項	8-209
Cisco Unified SIP SRST のセキュア SIP シグナリングおよび SRTP メディアのサポートについて	8-210
Cisco Unified Communications Manager の設定	8-210
電話の設定	8-211
セキュア SIP SRST の SIP オプションの設定	8-212
SIP SRST セキュリティ ポリシーの設定	8-213
セキュア SIP SRST の SIP ユーザ エージェントの設定	8-214
Cisco Unified SIP SRST の設定例	8-217
その他の関連資料	8-223
関連資料	8-223
標準	8-223
MIB	8-223
RFC	8-223
テクニカル サポート	8-224
コマンド リファレンス	8-224
セキュア SCCP および SIP SRST の機能情報	8-224
次の作業	8-225
Unified SRST での SIP トランキングの設定	9-227
目次	9-227
Unified SRST と Unified Border Element のコロケーション	9-227
Unified SRST と Unified Border Element のコロケーションの設定推奨	9-229
制限事項	9-231
例	9-231
Unified SRST での SIP トランキングの設定についての機能情報	9-240
ボイスメールと Cisco Unified SRST の統合	10-243
目次	10-243
ボイスメールの統合について Cisco Unified SRST	10-243
ボイスメールと Cisco Unified SCCP および SIP SRST との統合方法	10-245
ボイスメールへのダイレクト アクセスの設定	10-245

例	10-248	
メッセージ ボタンの設定	10-248	
例	10-250	
Cisco Unified Communications Manager ゲートウェイへのリダイレクト		10-250
ボイスメールへのコール転送の設定	10-251	
DTMF デジタル パターンを使用したコールのルーティング方法		10-251
前提条件	10-253	
例	10-255	
メッセージ待機インジケータの設定 (Cisco Unified SRST ルータ)		10-255
メッセージ待機インジケータの設定 (SRST モードの SIP 電話)		10-257
Unified SRST の設定例	10-259	
ローカル ボイスメール システム (FXO および FXS) の設定: 例		10-259
中央ボイスメール システム (FXO および FXS) の設定: 例		10-260
FXO および FXS 経由でのボイスメールへのアクセスの設定: 例		10-260
BRI および PRI 経由でのボイスメールへのアクセスの設定: 例		10-261
SIP SRST のメッセージ待機インジケータ: 例		10-261
SIP アプリケーションとボイスメールに DTMF リレーを設定する方法		10-262
SIP RFC 2833 を使用した DTMF リレー	10-262	
トラブルシューティングのヒント	10-264	
SIP NOTIFY を使用した DTMF リレー (非標準)	10-264	
トラブルシューティングのヒント	10-265	
次の作業	10-265	
ビデオ パラメータの設定	11-267	
目次	11-267	
ビデオ パラメータを設定するための前提条件	11-267	
ビデオ パラメータの設定に関する制約事項	11-268	
ビデオ パラメータの設定に関する情報	11-269	
エンドポイント機能の照合	11-269	
ビデオ コーデック情報の取得	11-269	
音声専用コールへのフォールバック	11-269	
ビデオ エンドポイント用のコールセットアップ	11-270	
2 つのローカル SCCP エンドポイント間でのコールセットアップ		11-270
SCCP および H.323 エンドポイント間でのコールセットアップ		11-270
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セッ トアップ	11-271	
RTP ビデオ ストリームのフロー	11-271	
Cisco Unified SRST のビデオ パラメータの設定方法	11-271	
Slow Connect プロシージャの設定	11-272	

Cisco Unified SRST の確認	11-272
例	11-273
Cisco Unified SRST のビデオ パラメータの設定	11-279
例	11-279
Cisco Unified SRST のトラブルシューティング	11-280
次の作業	11-280
Cisco Unified SRST のモニタリングとメンテナンス	12-281
リダイレクトモードを使用する Cisco Unified SIP SRST 機能の設定	A-1
目次	A-1
リダイレクトモードを使用する Cisco Unified SIP SRST 機能の前提条件	A-1
リダイレクトモードを使用する Cisco Unified SIP SRST 機能の制約事項	A-1
リダイレクトモードを使用する Cisco Unified SIP SRST 機能に関する情報	A-2
リダイレクトモードを使用する Cisco Unified SIP SRST 機能の設定方法	A-2
Cisco Unified SIP SRST 対応の SIP IP Phone 間のコールをサポートするためのコールリダイレクト拡張機能の設定	A-2
コールをグローバルにサポートするためのコールリダイレクト拡張機能の設定	A-3
特定の VoIP ダイアル ピアでコールをサポートするためのコールリダイレクト拡張機能の設定	A-4
300 Multiple Choice 送信のサポートの設定	A-5
リダイレクトモードを使用する Cisco Unified SIP SRST 機能の設定例	A-6
Cisco Unified SIP SRST: 例	A-7
次の作業	A-8
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-9
目次	B-9
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	B-10
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うえでの制約事項	B-10
Cisco Unified SRST ゲートウェイのマルチキャスト MOH リソースとしての使用に関する情報	B-11
Cisco Unified SRST ゲートウェイと Cisco Unified Communications Manager	B-11
コーデック、ポート番号、および IP アドレス	B-12
マルチキャスト MOH 伝送	B-14
ライブ フィードからの MOH	B-14
フラッシュ ファイルからの MOH	B-15

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	B-16
Cisco Unified Communications Manager を Cisco Unified SRST マルチキャスト MOH 対応に設定	B-16
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	B-18
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	B-19
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	B-21
MOH サーバの領域の作成	B-23
Cisco Unified Communications Manager マルチキャスト MOH の確認	B-24
Cisco Unified SRST をオーディオ ファイルからのマルチキャスト MOH に対応す るよう設定	B-25
前提条件	B-26
Cisco Unified SRST ゲートウェイでのマルチキャスト MOH の有効化	B-26
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	B-29
PSTN への Cisco Unified SRST MOH の確認	B-30
IP Phone への Cisco Unified SRST マルチキャスト MOH の確認	B-34
トラブルシューティングのヒント	B-34
Cisco Unified SRST をライブ フィードからの MOH に対応するよう設定	B-35
前提条件	B-36
制約事項	B-36
Cisco Unified SRST ゲートウェイの音声ポートの設定	B-36
Cisco Unified SRST ゲートウェイでの電話番号の設定	B-37
MOH フィードの確立	B-38
Cisco Unified SRST MOH ライブ フィードの確認	B-40
Cisco Unified SRST ゲートウェイの設定例	B-40
2 つの IP アドレスにルーティングされる MOH: 例	B-40
MOH ライブ フィード: 例	B-40
マルチキャスト MOH リソースとしての Cisco Unified SRST の機能情報	B-41
次の作業	B-41



はじめに

ここでは、『Cisco Unified SCCP および SIP SRST システム管理者ガイド』の対象読者と表記法について説明します。また、入手可能な製品ドキュメントを示し、ドキュメントの入手方法およびテクニカルサポートの利用方法についても説明します。

- [対象読者 \(i ページ\)](#)
- [表記法 \(i ページ\)](#)
- [マニュアルの入手方法およびテクニカルサポート \(ii ページ\)](#)

対象読者

このガイドの主な対象読者は、ネットワーク管理者およびチャネルパートナーです。

表記法

このマニュアルでは、次の表記法を使用しています。

項目	表記法
コマンドおよびキーワード。	太字フォント
ユーザが値を指定する変数。	イタリック体フォント
省略可能なコマンド キーワード。必ずしもオプションを選択する必要はありません。	[角カッコで囲む]
一連のオプションから選択する必須のコマンド キーワード。1 つのオプションを選択する必要があります。	{オプションを中カッコで囲み (縦棒) で区切る}
セッション情報およびシステム情報の表示出力。	screen font
ユーザが入力する情報。	boldface screen font
ユーザが入力する変数。	<i>italic screen font</i>

項目	表記法
メニュー項目およびボタン名。	[boldface] フォント
メニュー項目の選択。	[オプション (Option)] > [ネットワーク設定 (Network Preferences)]



(注)

「注釈」です。



ヒント

「問題解決に役立つ情報」です。



注意

「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。



ワンポイントアドバイス

「時間の節約に役立つ操作」です。記述されている操作を実行すると時間を節約できます。



警告

読者に対する警告を意味します。人為ミスを予防するための注意事項が記述されています。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool (BST) の使用、サービス要求の送信、追加情報の収集の詳細については、『[What's New in Cisco Product Documentation](#)』を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元に直接送信するには、『[What's New in Cisco Product Documentation](#)』RSS フィードをご購読ください。RSS フィードは無料のサービスです。



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

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。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。<http://www.cisco.com/go/fn> から『Cisco Feature Navigator』にアクセスしてください。アクセスするには、Cisco.com のアカウントが必要です。アカウントをお持ちでない場合や、ユーザ名や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 [キャンセル (Cancel)] をクリックし、表示される説明に従ってください。

目次

- マニュアルの構成 (iv ページ)
- 機能のロードマップ (v ページ)
- Cisco Unified SRST の新機能について (xi ページ)
- 次の作業 (xliii ページ)

マニュアルの構成

このマニュアルは、表 iii-1 に示す章または付録で構成されています。

表 iii-1 Cisco Unified SRST の設定順序

章または付録	説明
Cisco Unified SRST 機能の概要 (1 ページ)	Cisco Unified SRST の概要について説明します。また、サポートされるプラットフォームおよび Cisco Unified IP Phone について説明します。さらに、Cisco Unified SIP SRST を設定する前に対処する必要のある前提条件や制約事項についても説明します。
ネットワークの設定 (53 ページ)	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。
Cisco Unified Enhanced Survivable Remote Site Telephony (31 ページ)	ネットワークで Cisco Unified Enhanced SRST 機能を設定する方法について説明します。
Cisco Unified SIP SRST 4.1 (65 ページ)	Cisco Unified SIP SRST バージョン 4.1 の機能について説明します。また、関連する設定手順を示します。
SCCP を用いた Cisco Unified IP Phone の設定 (75 ページ)	Cisco Unified SRST Phone の基本的な設定方法について説明します。
SIP を用いた Cisco Unified IP Phone の設定 (93 ページ)	バージョン 3.4 にも必要な、バージョン 3.0 で使用できる機能について説明します。これらの説明には、基本的なレジストラ サービスを実装して外部 SIP プロキシサーバへのバックアップを実現するための手順が含まれます。これらのサービスは、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 IP Phone によって使用されます。
コール処理の設定 (109 ページ)	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。
SCCP および SIP のセキュア SRST の設定 (163 ページ)	Cisco Unified SRST に対するセキュア SRST セキュリティ機能について説明します。
ボイスメールと Cisco Unified SRST の統合 (243 ページ)	ボイスメールの設定方法について説明します。
ビデオパラメータの設定 (267 ページ)	ビデオパラメータの設定方法について説明します。
Cisco Unified SRST のモニタリングとメンテナンス (281 ページ)	Cisco Unified SRST のモニタリングとメンテナンスに有用な show コマンドのリストを示します。
リダイレクトモードを使用する Cisco Unified SIP SRST 機能の設定 (1 ページ)	バージョン 3.0 のみに適用される、リダイレクトモードを使用する機能について説明します。
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 (9 ページ)	Cisco Unified CM および Cisco Unified SRST を設定してマルチキャスト保留音 (MOH) を有効にする方法について説明します。

機能のロードマップ

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

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

Cisco Unified SRST	Cisco IOS Release	機能拡張または変更内容
バージョン 12.2	Cisco IOS XE Fuji 16.8.1	<ul style="list-style-type: none"> ボイス ハント グループのサポートがある Unified E-SRST (32 ページ)
バージョン 12.1	Cisco IOS XE Fuji 16.7.1	<ul style="list-style-type: none"> Cisco Smart License (14 ページ) Cisco 4000 シリーズ サービス統合型ルータでのセキュア SRST サポート (166 ページ) Unified SRST と Unified Border Element のコロケーション (227 ページ)
バージョン 12.0	Cisco IOS XE Everest 16.6.1	<ul style="list-style-type: none"> Unified SRST SIP IP Phone の IPv6 サポート (19 ページ)
バージョン 11.0	15.6(1)T	<ul style="list-style-type: none"> Cisco IP Phone 7811 のサポート Cisco IP Phone 8811, 8831, 8841, 8845, 8865, 8851, 8851NR, 8861 のサポート Cisco ATA-190 Phone のサポート
バージョン 10.5	15.4(3)M	<ul style="list-style-type: none"> Unified E-SRST のスケール サポート (51 ページ) Cisco Unified DX650 SIP IP Phone のサポート (xii ページ) Cisco Unified 78xx SIP IP Phone のサポート (xii ページ) Cisco IP Phone 88xx, 8941, 8945, および 8961 のサポート
バージョン 10.0	15.3(3)M	<ul style="list-style-type: none"> Cisco Jabber for Windows (xiii ページ) SIP: Unified E-SRST の設定 (35 ページ) Cisco.com のアカウントを取得するには、www.cisco.com に移動し、画面上部の [登録 (Register)] をクリックします。(4 ページ)
バージョン 9.5	15.3(2)T	<ul style="list-style-type: none"> after-hours パターンブロッキングでの正規表現のサポート (xiv ページ) コール パークの再コールの機能拡張 (xv ページ) コールされたボイス ハント グループの名前の表示のサポート (xvi ページ) ボイス ハント グループの最終エージェントへのローカル コール転送の防止 (xvii ページ) Cisco Unified SIP IP Phone における、電話料金詐欺行為防止を目的としたトランク間転送ブロッキング (xvii ページ)
バージョン 9.1	15.2(4)M	<ul style="list-style-type: none"> Cisco Unified SIP IP Phone の KEM のサポート (xxv ページ) スピード ダイアル サポートの機能強化 (xxv ページ) ボイス ハント グループのサポート (xxvi ページ)

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

Cisco Unified SRST	Cisco IOS Release	機能拡張または変更内容
バージョン 9.0	15.2(2)T	<ul style="list-style-type: none"> • Cisco Unified 6901 および 6911 SIP IP Phone のサポート (xxvii ページ) • Cisco Unified 6921、6941、6945、および 6961 SIP IP Phone のサポート (xxvii ページ) • Cisco Unified 8941 および 8945 SIP IP Phone のサポート (xxvii ページ) • 回線ごとの複数コール (xxvii ページ) • Cisco ATA-187 での音声とファクスのサポート (xxviii ページ)
バージョン 8.8	15.2(1)T	Cisco Unified 6945、8941、および 8945 SCCP IP Phone のサポート (xxviii ページ)
バージョン 8.6	15.1(4)M	Cisco Unified 8941 および 8945 SCCP IP Phone のサポートが導入されました。詳細については、Cisco Unified 8941 および 8945 SCCP IP Phone の設定 (78 ページ) を参照してください。
バージョン 8.0	15.1(1)T	<p>Cisco IP Phone ファームウェア 8.5(3) および Cisco IOS リリース 15.1(1)T 以降、Cisco SRST は、RTP と SRTP の両方のメディア接続が IP Phone のセキュリティ設定に基づいている場合に、UDP、TCP、および TLS 接続を介した SIP シグナリングをサポートします。詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> • Unified SRST でのシグナリングのセキュリティ (TLS) (167 ページ) • Unified SRST でのメディアのセキュリティ (SRTP) (169 ページ) • Cisco SRST でのセキュアな SIP コールシグナリングおよび SRTP メディアの設定 (209 ページ)
バージョン 7.0/4.3	互換性については『Cisco Feature Navigator』を参照してください。	<ul style="list-style-type: none"> • 各ボタンで 8 つのコールの設定 (オクトライン) (87 ページ) • コンサルタティブ転送の設定 (120 ページ)
バージョン 4.2(1)	互換性については『Cisco Feature Navigator』を参照してください。	<p>Enhanced 911 サービス (69 ページ)</p> <p>次の新機能が含まれます。</p> <ul style="list-style-type: none"> • 発信者に最も近い PSAP にルーティングするための、ゾーンに対する ERL の割り当て。 • デフォルト ELIN の定義と、911 発信者がコールバックに到達できない場合における指定番号の特定と、最終発信者テーブルにあるデータの期限切れ時間の指定と、すべての緊急コールを伝達する syslog メッセージのイネーブル化とによる、E911 のカスタマイズ。 • 名前およびアドレスを含む、E911 位置情報の拡張。 • 新しい永続的なコール詳細レコードの追加。
バージョン 4.1	12.4(15)T	<ul style="list-style-type: none"> • SIP 電話の KPML の有効化 (69 ページ) • コール自動転送およびコール転送の SIP 補足サービスのディセーブル化 (68 ページ) • SIP 電話のアイドルプロンプトステータスの設定 (72 ページ) • Enhanced 911 サービス (69 ページ)

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

Cisco Unified SRST	Cisco IOS Release	機能拡張または変更内容
バージョン 4.0	12.4(4)XC	<ul style="list-style-type: none"> • Cisco IP Communicator のサポート (xxx ページ) • SCCP および ATA サポートを使用した FAX パススルー (xxx ページ) • 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 (SCCP 電話) (xxx ページ) • ビデオ サポート (xxxi ページ)
バージョン 3.4	12.4(4)T	<ul style="list-style-type: none"> • Cisco SIP SRST 3.4 (xxxi ページ) • リダイレクトモードを使用する Cisco Unified SIP SRST 機能の設定 (1 ページ) • コール処理の設定 (109 ページ) (「バックツーバック ユーザーエージェントモード」を参照)
バージョン 3.3		<ul style="list-style-type: none"> • セキュア SRST (xxxi ページ) • Cisco Unified IP Phone 7970G および Cisco Unified 7971G-GE のサポート (xxxii ページ) • show ephone コマンドの機能拡張 (xxxii ページ)
バージョン 3.2	12.3(11)T	<ul style="list-style-type: none"> • alias コマンドの機能拡張 (xxxiii ページ) • pickup コマンドの機能拡張 (xxxiii ページ) • user-locale コマンドの機能拡張 (xxxiii ページ) • Cisco 3845 でサポートされる Cisco Unified IP Phone の台数増加 (xxxiii ページ) • MOH ライブフィードのサポート (xxxiv ページ) • コールプリザベーションのタイムアウトなし (xxxiv ページ) • RFC 2833 DTMF リレーのサポート (xxxiv ページ) • トランスレーションプロファイルのサポート (xxxiv ページ)
バージョン 3.1	12.3(7)T	<ul style="list-style-type: none"> • Cisco Unified IP Phone 7920 のサポート (xxxv ページ) • Cisco Unified IP Phone 7936 のサポート (xxxv ページ)

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

Cisco Unified SRST	Cisco IOS Release	機能拡張または変更内容
バージョン 3.0	12.2(15)ZJ 12.3(4)T	<ul style="list-style-type: none"> IP Phone のディスプレイに対する追加の言語オプション(xxxvi ページ) 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 (SCCP 電話) (xxxvi ページ) Cisco Unified IP Phone 用にカスタマイズされたシステム メッセージ (xxxvi ページ) 二重回線モード(xxxvii ページ) E1 R2 シグナリングのサポート(xxxvii ページ) 欧州の日付形式(xxxviii ページ) 二重回線モードのハントストップ(xxxviii ページ) フラッシュ ファイルからのマルチキャスト用の保留音(xxxviii ページ) 呼び出しタイムアウトのデフォルト(xxxix ページ) 2 次ダイヤルトーン(xxxix ページ) show ephone コマンドの機能拡張(xxxix ページ) 電話機の登録に関するシステム ログ メッセージ(xxxix ページ) 3 者間の G.711 アドホック会議(xxxix ページ) Cisco VG248 Analog Phone Gateway 1.2(1) 以降のバージョンのサポート (xxxix ページ)
バージョン 2.1		<ul style="list-style-type: none"> Cisco Unified IP Phone 7902G のサポート(xli ページ) Cisco Unified IP Phone 7912G のサポート(xli ページ) IP Phone のディスプレイに対する追加の言語オプション(xl ページ) Cisco SRST の集約(xli ページ) Cisco ATA 186 および ATA 188 のサポート(xli ページ) Cisco Unified IP Phone 7905G のサポート(xli ページ) Cisco Unified IP Phone 7914 拡張モジュールのサポート(xlii ページ) dialplan-pattern コマンドの機能拡張(xlii ページ)
バージョン 2.02		<ul style="list-style-type: none"> Cisco Unified IP Phone Conference Station 7935 のサポート(xlii ページ) 電話番号の増加(xliii ページ) 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(xliii ページ) Cisco Unified SRST が Cisco Catalyst 4500 Access Gateway Module および Cisco 7200 ルータ (NPE-225、NPE-300、および NPE400) に実装されました。 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。
バージョン 2.01		<ul style="list-style-type: none"> 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。 追加接続された Cisco IP Phone もサポートされるようになりました。 Cisco IP Phone 上における、追加の電話番号または仮想音声ポートもサポートされるようになりました。

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

Cisco Unified SRST	Cisco IOS Release	機能拡張または変更内容
バージョン 2.0		<ul style="list-style-type: none"> • Cisco Unified SRST が Cisco 2600XM および Cisco 2691 ルータに実装されました。 • Cisco Unified SRST が Cisco IOS リリース 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。 • Cisco Unified SRST が Cisco 1750 および Cisco 1751 ルータに実装されました。 • ハントストップのサポート • 制限クラス (COR) • トランスレーション ルールのサポート • MOH と保留トーン • 特殊呼出音 • 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自動応答 (AA) への転送。 • 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。 • 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。

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

Cisco Unified SRST	Cisco IOS Release	機能拡張または変更内容
バージョン 1.0		<ul style="list-style-type: none"> • 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。 • 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 Series Integrated Access Devices に導入されました。 • 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。 • Cisco Unified SRST の動作中、サポートされない Cisco Unified IP Phone のファンクション キーはすべてグレー表示されるようになりました。 • 内線間ダイヤル • ダイヤルイン方式(DID) • ダイヤルアウト方式(DOD) • 発信側 ID(発信者 ID/ANI)の表示 • 最後にかけた番号へのリダイヤル • WAN リンクの障害時における、ローカル内線間コールの保持。 • WAN リンクの障害時における、ローカル内線と PSTN の間のコールの保持。 • 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。 • IP ネットワークにおけるコールのブラインド転送。 • Cisco IP Phone ごとの複数回線 • 電話機全体での複数回線通話 • コール保留(共有回線) • アナログ Foreign Exchange Station (FXS) および Foreign Exchange Office (FXO) ポート • EuroISDN の BRI サポート • NET5 スイッチ タイプの PRI サポート

Cisco Unified SRST の新機能について

ここでは、次の項目について説明します。

- [Unified SRST バージョン 12.1 の新機能 \(xi ページ\)](#)
- [Unified SRST バージョン 12.0 の新機能 \(xi ページ\)](#)
- [Cisco Unified SRST バージョン 11.0 の新機能 \(xii ページ\)](#)
- [Cisco Unified SRST バージョン 10.5 の新機能 \(xii ページ\)](#)
- [Cisco Unified SRST バージョン 10.0 の新機能 \(xii ページ\)](#)
- [Cisco Unified SRST バージョン 9.5 の新機能 \(xiii ページ\)](#)
- [Cisco Unified SRST バージョン 9.1 の新機能 \(xxiv ページ\)](#)
- [Cisco Unified SRST バージョン 9.0 の新機能 \(xxvi ページ\)](#)
- [Cisco Unified SRST バージョン 8.8 の新機能 \(xxviii ページ\)](#)
- [Cisco Unified SRST バージョン 8.0 の新機能 \(xxviii ページ\)](#)
- [Cisco Unified SRST バージョン 7.0/4.3 の新機能 \(xxix ページ\)](#)
- [Cisco Unified SRST バージョン 4.2\(1\) の新機能 \(xxix ページ\)](#)
- [Cisco Unified SRST バージョン 4.1 の新機能 \(xxix ページ\)](#)
- [Cisco Unified SRST バージョン 4.0 の新機能 \(xxix ページ\)](#)
- [Cisco Unified SRST バージョン 3.4 の新機能 \(xxxi ページ\)](#)
- [Cisco SRST バージョン 3.3 の新機能 \(xxxii ページ\)](#)
- [Cisco SRST バージョン 3.2 の新機能 \(xxxii ページ\)](#)
- [Cisco SRST バージョン 3.1 の新機能 \(xxxv ページ\)](#)
- [Cisco SRST バージョン 3.0 の新機能 \(xxxv ページ\)](#)
- [Cisco SRST バージョン 2.1 の新機能 \(xl ページ\)](#)
- [Cisco SRST バージョン 2.02 の新機能 \(xlii ページ\)](#)

Unified SRST バージョン 12.1 の新機能

Unified SRST 12.1 では、次の新機能のサポートが導入されています。

- [Cisco Smart License \(14 ページ\)](#)
- [Cisco 4000 シリーズ サービス統合型ルータでのセキュア SRST サポート \(166 ページ\)](#)
- [Unified SRST と Unified Border Element のコロケーション \(227 ページ\)](#)

Unified SRST バージョン 12.0 の新機能

Cisco Unified SRST 12.0 は SIP IP フォンでの IPv6 プロトコルのサポートを導入しています。Unified SRST に導入された IPv6 サポートの詳細については、[Unified SRST SIP IP Phone の IPv6 サポート \(19 ページ\)](#) を参照してください。

Cisco Unified SRST バージョン 11.0 の新機能

Cisco Unified SRST 11.0 では、次の新しい Cisco IP Phone およびアダプタがサポートされています。

- Cisco IP Phone 7811 のサポート
- Cisco IP Phone 8811、8831、8841、8851、8851NR、8861 のサポート
- Cisco ATA-190 のサポート

Cisco Unified SRST 11.0 でサポートされている電話機については、『[Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST](#)』を参照してください。

Cisco Unified SRST バージョン 10.5 の新機能

Cisco Unified SRST 10.5 では、次の機能がサポートされています。

- [Unified E-SRST のスケール サポート \(51 ページ\)](#)

Cisco Unified SRST 10.5 でサポートされている機能の詳細については、『[SCCP: Unified E-SRST の設定](#)』セクション (50 ページ) を参照してください。

Cisco Unified SRST 10.5 では、次の新しい Cisco Unified SIP IP Phone がサポートされています。

- [Cisco Unified DX650 SIP IP Phone のサポート \(xii ページ\)](#)
- [Cisco Unified 78xx SIP IP Phone のサポート \(xii ページ\)](#)

Cisco Unified DX650 SIP IP Phone のサポート

Cisco Unified SRST 10.5 での Cisco Unified DX650 SIP IP Phone 関連の機能サポートについては、『[Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST](#)』を参照してください。

Cisco Unified 78xx SIP IP Phone のサポート

Cisco Unified SRST 10.5 での Cisco Unified 78xx SIP IP Phone 関連の機能サポートについては、『[Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST](#)』を参照してください。

Cisco Unified SRST バージョン 10.0 の新機能

Cisco Unified SRST 10.0 では、次の新機能がサポートされています。

- [Cisco Jabber for Windows \(xiii ページ\)](#)
- [SIP: Unified E-SRST の設定 \(35 ページ\)](#)
- Cisco.com のアカウントを取得するには、www.cisco.com に移動し、画面上部の [登録 (Register)] をクリックします。

Cisco Jabber for Windows

Cisco Jabber for Windows クライアントは、Cisco Unified CME リリース 10 以降でサポートされています。Cisco Jabber for Windows は、Cisco Unity Connection と統合されるビジュアルボイスメール機能をサポートしています。Cisco Jabber for Windows は、インスタントメッセージおよびプレゼンス機能と統合される SIP ベースのソフトクライアントで、新しいクライアント サービス フレームワークの第 2 世代 (CSF2G) アーキテクチャを採用しています。

CSF は、複数の PC 向け Cisco クライアントによって繰り返し使用されるユニファイド コミュニケーション エンジンです。Cisco Jabber クライアントで標準 XMPP ベース インスタントメッセージ機能を利用するには、クライアントがプレゼンス サーバ (クラウドベースの Cisco WebEx サーバ、Cisco Unified Presence サーバなど) に登録されている必要があります。クライアントは、Cisco Unified CME の音声レジスタ プールで設定できるデバイス ID 名で識別されます。Cisco Jabber for Windows クライアントを使用して Cisco Unified CME にログインしているユーザを識別するには、音声レジスタ プールでユーザ名とパスワードを設定する必要があります。デバイス検出プロセスには HTTPS 接続が使用されます。したがって、Cisco Unified CME 上でセキュア HTTP を設定する必要があります。Cisco Jabber for Windows クライアントに関連して、音声レジスタ プールを設定するための「Jabber-Win」という新しい電話機タイプが追加されました。

制約事項

- Cisco Jabber for Windows クライアントは、バージョン 9.1.0 以降である必要があります。
- Cisco Jabber for Windows クライアントでテレフォニー機能を有効にするには、Jabber クライアントがプレゼンス サーバ (クラウドベースの WebEx サーバ、Cisco Unified Presence サーバなど) に登録されている必要があります。
- Cisco Jabber for Windows クライアントは、Cisco Unity Connection での Internet Message Access Protocol (IMAP) によるビジュアルボイスメール機能のみをサポートします。
- Cisco Jabber for Windows クライアントは、ソフトウェアベースの電話会議をサポートせず、Cisco Unified CME によるソフトフォンモードのみをサポートします。
- デスクフォンモデルはサポートされません。

設定については、『[Cisco Unified Communications Manager Administration Guide](#)』の「Cisco Jabber for Windows」のセクションを参照してください。

Cisco Unified SIP IP Phone のバージョン ネゴシエーション

Cisco Unified SIP IP Phone のバージョン ネゴシエーションが Cisco Unified SRST 10.0 リリースで導入されました。Cisco Unified SRST 10.0 でサポートされている機能の詳細については、『[SIP: Unified E-SRST の設定](#)」セクション (35 ページ) を参照してください。

Cisco Unified SRST バージョン 9.5 の新機能

Cisco Unified SRST 9.5 では、次の新機能がサポートされています。

- [after-hours パターン ブロッキングでの正規表現のサポート](#) (xiv ページ)
- [コール パークの再コールの機能拡張](#) (xv ページ)
- [コールされたボイス ハント グループの名前の表示のサポート](#) (xvi ページ)

- ボイス ハント グループの最終エージェントへのローカル コール転送の防止 (xvii ページ)
- Cisco Unified SIP IP Phone における、電話料金詐欺行為防止を目的としたトランク間転送ブロッキング (xvii ページ)

after-hours パターンブロッキングでの正規表現のサポート

Cisco Unified SRST 9.5 では、Cisco Unified SIP および Cisco Unified SCCP IP Phone でのダイヤルプランに関して、after-hours パターンブロッキングのサポートが正規表現パターンに拡張されました。これにより、固定ダイヤルプランと正規表現ベースのダイヤルプランを組み合わせる追加できます。

指定期間にコールが開始されると、着信番号がダイヤルプランの組み合わせと照合されます。一致する場合は、コールがブロックされます。

after-hours パターンブロッキングの設定時に正規表現パターンを含めるには、**after-hours block pattern** コマンドを修正して、次のコマンド構文で正規表現を *pattern* 引数の値に追加します。

after-hours block pattern pattern-tag pattern

このコマンドは、次のコンフィギュレーションモードで使用できます。

- telephony-service: SCCP 電話と SIP 電話の両方
- ephone-template: SCCP 電話のみ



(注) 正規表現パターンの最大長は、Cisco Unified SIP IP Phone と Cisco Unified SCCP IP Phone のどちらの場合も 32 です。

たとえば、指定期間の次の番号へのコールをブロックするとします。

- 「0」と「00」で始まる番号
- 「1800」で始まり、その後 4 桁の数字が続く番号
- 9876512340 ~ 9876512345 の番号

この場合は、次の設定を使用できます。

- after-hours block pattern 1 0*
- after-hours block pattern 2 00*
- after-hours block pattern 3 1800....
- after-hours block pattern 4 987651234[0-5]



(注) 追加できる after-hours パターンの数に変更はありません。最大数は 100 のままです。

設定例の詳細については、『[Cisco Unified Communications Manager Administration Guide](#)』の「[Configuring Afterhours Block Patterns of Regular Expressions: Example](#)」のセクションを参照してください。

基本的な Cisco IOS の正規表現の文字と機能の概要については、『[Terminal Services Configuration Guide](#)』の「[Cisco Regular Expression Pattern Matching Characters](#)」のセクションを参照してください。

コールパークの再コールの機能拡張

Cisco Unified CME 9.5 の前は、コールをパーク保留した電話機や、宛先の電話機がオフフック/呼び出し中のときにコールを転送した当初の電話機について、パーク保留中の再コールを再発信したり、転送先に指定したりすることはできませんでした。

Cisco Unified CME 9.5 では、telephony-service コンフィギュレーションモードの **call-park system** コマンドに **recall force** キーワードが追加されました。これにより、宛先の電話機がコールに応答できるときに、コールをパーク保留した電話機や予約対象番号をプライマリ電話番号とする電話機に対して、パーク保留中のコールを再コールさせたり、転送先に指定したりすることが可能になりました。

Cisco Unified CME 10.5 では、電話機ユーザがコールのタイプをはっきりと識別できるように、パーク保留の再コールを表す新しい着信音が導入されました。

この機能は、SCCP エンドポイント用のすべての電話機ファミリと SIP エンドポイント用の 89XX および 99XX 電話機ファミリでサポートされます。この機能を有効にするために設定する必要はありません。

例

次の例では、コールパークの再コールを設定します。

```
Router# configure terminal
Router(config)# telephony-service
Router(config)# srst mode auto-provision all
Router(config-telephony)# call-park system ? recall Configure parameters for recall
Router(config-telephony)# call-park system recall ? force Force recall for busy call park
initiator
Router(config-telephony)# call-park system recall force
```

パーク モニタリング

In Cisco Unified CME 8.5 以降のバージョンでは、パーク モニタリング機能で、パーク中のコールが取得または破棄されるまでコールをパークし、パーク中のコールのステータスをモニタすることができます。Cisco Unified SIP IP Phone 8961、9951、または 9971 は [パーク (Park)] ソフトキーを使用してコールをパークし、パーク モニタリング機能はパーク中のコールのステータスをモニタします。パーク中のコールが取得されるか、またはパーク取得者によって破棄されるまで、パーク モニタリング コール バブルはクリアされません。このパーク中のコールは、パーク元の電話機で同じコール バブルを使用して取得でき、パーク中のコールのステータスをモニタできます。

コールがパークされると、Cisco Unified CME は SIP NOTIFY メッセージをパーク元の電話機に送信します。このメッセージは、コールがパークされている間にパーク元の電話機でパーク スロット番号を表示できるように、「パークされた」イベントとパーク スロット番号を示します。

パーク中のコールが取得されると、Cisco Unified CME は別の SIP NOTIFY メッセージをパーク元の電話機に送信します。このメッセージは、この電話機でコール バブルをクリアできるように、「取得された」イベントを示します。パーク中のコールが取得者によって接続解除されると、Cisco Unified CME は SIP NOTIFY メッセージをパーク元の電話機に送信します。このメッセージはイベントが「破棄された」ことを示し、パーク元の電話機はパーク中のコールのキャンセル時にコール バブルをクリアします。

パーク中のコールが再呼出または転送されると、Cisco Unified CME は SIP NOTIFY メッセージをパーク元の電話機に送信します。このメッセージは、イベントが「転送された」ことを示します。これにより、パーク元の電話機では、パーク、再呼出、および転送の実行時にコールバブルをクリアできます。また、パーク元の電話機から直接コールバブルを選択するか、または電話機で [復帰 (Resume)] ソフトキーを押して、パーク中のコールを取得できます。

コールされたボイス ハント グループの名前の表示のサポート

ボイス ハント グループはパイロット番号に関連付けられます。ただし、コールがボイス ハント グループから最終番号に転送される場合は、ボイス ハント グループの名前の関連付けがないため、転送番号が転送側の名前なしで送信されます。最終番号は、ボイスメール、基本自動着信呼分配 (BACD) スクリプト、または別の内線の形式である場合があります。

Cisco Unified SRST 9.5 では、voice hunt-group または ephone-hunt コンフィギュレーション モードで次のコマンドを設定することにより、コールされたボイス ハント グループ パイロットの名前の表示がサポートされます。

```
[no] name "primary pilot name" [secondary "secondary pilot name"]
```

セカンダリ名はオプションです。セカンダリ パイロット名を明示的に設定しない場合は、プライマリ パイロット名が両方のパイロット番号に適用されます。

設定については、「Associating a Name with a Called Voice Hunt Group」のセクションを参照してください。

例

次の例では、プライマリ パイロット番号とセカンダリ パイロット番号の両方のプライマリ パイロット名を設定します。

```
name SALES
```

次の例では、プライマリ パイロット番号とセカンダリ パイロット番号にそれぞれ異なる名前を設定します。

```
name SALES secondary SALES-SECONDARY
```



(注)

以下の 3 つの例のように、入力文字列にスペースが含まれている場合は引用符 (") を使用します。

次の例では、プライマリ パイロット番号の 2 語の名前とセカンダリ パイロット番号の 1 語の名前を関連付けます。

```
name "CUSTOMER SERVICE" secondary CS
```

次の例では、プライマリ パイロット番号の 1 語の名前とセカンダリ パイロット番号の 2 語の名前を関連付けます。

```
name FINANCE secondary "INTERNAL ACCOUNTING"
```

次の例では、プライマリ パイロット番号とセカンダリ パイロット番号の 2 語の名前を関連付けます。

```
name "INTERNAL LLER" secondary "EXTERNAL LLER"
```


設定については、『[Cisco Unified Communications Manager Administration Guide](#)』の「Associating a Name with a Called Voice Hunt Group」のセクションを参照してください。

設定例については、『[Cisco Unified Communications Manager Administration Guide](#)』の「Example: Associating a Name with a Called Voice Hunt Group」のセクションを参照してください。

制約事項

- 表示のサポートは、voice hunt-group および ephone-hunt コンフィギュレーション モードの Cisco Unified SCCP IP Phone に適用されますが、Cisco Unified SIP IP Phone ではサポートされません。
- 発信者の電話機に表示される着信者名および着信者番号の情報は、既存の動作に従います。つまり、着信者名および着信者番号が更新されることで、シーケンシャル ハントに呼び出し中の電話機の名前と番号が反映されます。

ボイス ハント グループの最終エージェントへのローカル コール転送の防止

ローカル コール(または内部コール)とは、同じ Cisco Unified CME システム内の Cisco Unified SIP Phone または Cisco Unified SCCP IP Phone から発信されるコールです。

Cisco Unified CME 9.5 よりも前は、ローカル コールが次のエージェントに転送されることを防止するため、ephone-hunt グループで **no forward local-calls** コマンドが設定されていました。

Cisco Unified CME 9.5 では、parallel voice hunt-group または sequential voice hunt-group コンフィギュレーション モードで **no forward local-calls to-final** コマンドを使用することにより、ローカル コールの最終宛先への転送が防止されます。

sequential voice hunt-group コンフィギュレーション モードで **no forward local-calls to-final** コマンドが設定されている場合、ハント グループ パイロット番号へのローカル コールは、ロータリー ハント手法を使用してグループのメンバーのリストにのみシーケンシャルに送信されます。ボイス ハントグループのすべてのグループ メンバーが話中の場合、発信者には話中音が聞こえます。グループ メンバーのいずれかが応答可能であるのに応答しない場合、発信者にはリングバック トーンが流れます。最終的には、指定されたタイムアウト時間が経過すると切断されません。コールは最終番号には転送されません。

parallel voice hunt-group コンフィギュレーション モードで **no forward local-calls to-final** コマンドが設定されている場合、ハント グループ パイロット番号へのローカル コールは、ブラスト手法を使用してグループのメンバーのリストに同時に送信されます。ボイス ハントグループのすべてのグループ メンバーが話中の場合、発信者には話中音が聞こえます。グループ メンバーのいずれかが応答可能であるのに応答しない場合、発信者にはリングバック トーンが流れます。最終的には、指定されたタイムアウト時間が経過すると切断されます。コールは最終番号には転送されません。設定例については、『[Cisco Unified Communications Manager Administration Guide](#)』の「Preventing Local-Call Forwarding to Final Agent in Voice Hunt Groups」のセクションを参照してください。

Cisco Unified SIP IP Phone における、電話料金詐欺行為防止を目的としたトランク間転送ブロック

Cisco Unified Survivable Remote Site Telephony (SRST) 4.0 では、電話料金詐欺行為を防止するためのトランク間転送ブロック機能が、Cisco Unified Skinny Client Control Protocol (SCCP) IP Phone でサポートされています。

表 iii-3 に、Cisco Unified CME および Cisco Unified SRST の転送ブロック コマンドと適切なコンフィギュレーション モードを示します。

表 iii-3 転送ブロッキングコマンドのコンフィギュレーションモード

コマンド	Cisco Unified SRST
transfer-pattern	call-manager-fallback
transfer max-length	voice register pool
transfer-pattern blocked	voice register pool
conference transfer-pattern	call-manager-fallback
conference max-length	voice register pool または voice register template
conference-pattern blocked	voice register pool または voice register template



(注)

転送または電話会議が PSTN トランク、SIP トランク、H.323 トランクなどの外部パーティに向けて開始されると、コール転送制限や電話会議制限が適用されます。これらの制限は、ローカル内線番号への転送および電話会議には適用されません。

transfer-pattern

Cisco Unified SIP IP Phone 機能の **transfer-pattern** コマンドは、ローカルだけでなくすべての転送の実行を許可する点で、Cisco Unified SCCP IP Phone の **transfer-pattern** コマンドと似ています。

transfer-pattern コマンドはコール転送の電話番号を指定します。このコマンドは、**transfer-pattern transfer-pattern [blind]** というコマンド構文により、最大 32 回設定できます。



(注)

transfer-pattern コマンド内の **blind** キーワードは、Cisco Unified SCCP IP Phone にのみ適用されます。Cisco Unified SIP IP Phone には適用されません。

transfer-pattern コマンドが設定されている場合、設定された転送パターンに一致する番号へのコール転送のみ、実行が許可されます。転送パターンが設定されている場合、すべてまたは一部の転送番号にダイヤルでき、リモートパーティへの転送を開始できます。

次に、設定可能な転送パターンの例を示します。

- 「.T」: この設定により、1 桁以上の番号 (123、877656、76548765 など) の接続先へのコール転送が許可されます。
- 「919.....」: この設定により、「919」で始まり、その後 8 桁の数字が続くリモート番号 (91912345678 など) へのコール転送のみが許可されます。したがって、9191234 や 919123456789 などのコール転送は許可されません。

下位互換性

下位互換性を維持するため、**transfer-pattern**、**transfer-pattern blocked**、または **transfer max-length** コマンドによって転送パターンが設定されていない場合について、Cisco Unified SIP IP Phone から任意の番号 (ローカルまたはトランク経由) へのコール転送はすべて許可されます。

Cisco Unified SCCP IP Phone については、転送パターンが設定されていなければ、トランク経由のコール転送が引き続きブロックされます。

ダイヤルプラン

外部コールに関して使用するダイヤルプランでは、**transfer-pattern** コマンドを使用することで、同じ番号を特定の番号として設定する必要があります。

外部コールを発信する前に「9」をダイヤルする必要があるダイヤルプランの場合は、「9」を転送パターン番号のプレフィックスに設定する必要があります。たとえば、12345678 が、外部コールを発信する前に「9」をダイヤルする必要がある外線番号である場合は、転送パターン番号を 912345678 にする必要があります。

transfer max-length

transfer max-length コマンドは、コール転送の際にダイヤルされる番号に対して最大長を指定します。コール転送時に特定の桁数のみを許可する場合は、3 ~ 16 の値を設定します。ダイヤルされる番号が、設定された最大長を超えると、コール転送がブロックされます。

たとえば、最大長が 5 に設定されている場合、Cisco Unified SIP IP Phone から最大 5 桁の電話番号へのコール転送のみが許可されます。5 桁を超える電話番号へのコール転送はすべてブロックされます。



(注) **transfer max-length** のみが設定されており、**conference max-length** が設定されていない場合、**transfer max-length** は転送と電話会議に適用されます。

transfer-pattern blocked

特定の電話機に **transfer-pattern blocked** コマンドが設定されている場合は、その電話機からトランク経由でコールを転送することは一切許可されません。

この機能により、特定の電話機から任意の別の非ローカル番号(あるトランクから別のトランクへの外部コール)へのコール転送はすべて無条件にブロックされます。転送パターンが転送先のダイヤル番号に適合する場合でも、この特定の電話機からのコール転送は許可されません。

表 iii-4 に、特定の設定に関する Cisco Unified SCCP IP Phone と Cisco Unified SIP IP Phone の動作の比較を示します。

表 iii-4 特定の設定に関する Cisco Unified IP Phone の動作

設定	Cisco Unified SCCP IP Phone	Cisco Unified SIP IP Phone
転送パターンが設定されていない。	すべての非ローカル コール転送がブロックされます。	下位互換性のため、すべての非ローカル コール転送が許可されます。
特定の転送パターンが設定されている。	特定の外部エンティティへのコール転送が許可されます。	特定の外部エンティティへのコール転送が許可されます。
transfer-pattern blocked コマンドが設定されている。	すべての非ローカル コール転送がブロックされます。 (注) この設定により、デフォルト(転送パターンが設定されていない状態)に戻ります。	すべての非ローカル コール転送がブロックされます。 (注) この設定により、すべての非ローカル コール転送が無条件でブロックされます。デフォルト(すべての非ローカル コール転送が許可される状態)には戻りません。

conference-pattern blocked

conference-pattern blocked コマンドは、音声レジスタ プールの内線番号から電話会議を開始することを防ぎます。

次の表に、**no conference-pattern blocked**、**conference max-length**、**no conference max-length**、および **transfer max-length** コマンドに関連した **conference-pattern blocked** コマンドの動作の概要を示します。

	conference max-length	no conference max-length
no conference-pattern blocked (デフォルトの場合)	電話会議の許可/ブロックは、設定された conference max-length によって決まります。	電話会議の許可/ブロックは、設定された transfer max-length によって決まります。
conference-pattern blocked	電話会議は SIP 電話および SCCP 電話では許可されません。	

	最大長が許可されており、かつ最大長以下の場合		最大長が許可されており、かつ最大長を超える場合	
	転送	会議	転送	会議
transfer max-length と no conference max-length (conference max-length が設定されていないため、電話会議の場合も transfer max-length を使用)	Y	Y	N	N
no transfer max-length と conference max-length (電話会議の場合は transfer max-length よりも conference max-length が優先される)	Y	Y	Y	N
no transfer max-length と conference max-length (電話会議の場合は transfer max-length よりも conference max-length が優先される)	Y	Y	N	N
no transfer max-length と no conference max-length	すべての転送と電話会議が許可されます。			

電話会議に対する最大桁数の設定

この機能により、電話会議の発信時における最大桁数を指定できます。

前提条件

- Cisco Unified SRST 10.5 以降のバージョン。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice register pool *pool-tag***
4. **conference max-length *value***
5. **end**

手順の詳細

	コマンドまたはアクション	目的
手順 1	enable 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	configure terminal 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	voice register pool <i>pool-tag</i> or ephone <i>phone-tag</i> 例: Router(config)# voice register pool 25	音声レジスタ プール コンフィギュレーション モードを開始し、Cisco Unified CME の Cisco Unified SIP IP Phone に対して、または Cisco Unified SIP SRST の一連の Cisco Unified SIP IP Phone に対してプール設定を作成します。 • <i>pool-tag</i> : プールに割り当てる一意の番号。範囲は 1 ~ 100 です。 または 音声レジスタ テンプレート コンフィギュレーション モードを開始し、Cisco Unified SIP IP Phone の共通パラメータのテンプレートを定義します。 • <i>template-tag</i> : テンプレート タグを宣言します。範囲は 1 ~ 10 です。 または ephone コンフィギュレーション モードを開始します。 <i>phone-tag</i> : 設定タスク中にこの ephone を識別する一意のシーケンス番号。 ephone の最大数はバージョンやプラットフォームによって異なります。範囲を表示するには、? と入力します。
手順 4	configure max-length <i>value</i> 例: Router(config-telephony)# conference max-length 6	Cisco IP Phone から、Cisco IP Phone 以外の電話機の指定された電話番号への電話会議コールが許可されます。 • <i>conference max-length</i> : 設定された conference max-length に応じて電話会議を許可します。範囲は 3 ~ 16 です。
手順 5	end 例: Router(config-telephony)# end	telephony-service コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

電話機で電話会議ブロッキング オプションを設定する

この機能は、内線から他の方法でグローバルに許可されている電話番号への電話会議の発信を防止します。

前提条件

- Cisco Unified SRST 10.5 以降のバージョン。
- `transfer-pattern` コマンドが設定されている必要があります。
- `conference transfer-pattern` コマンドが設定されている必要があります。

手順の概要

1. `enable`
2. `configure terminal`
3. `voice register pool pool-tag`
4. `conference-pattern blocked`
5. `end`

手順の詳細

	コマンドまたはアクション	目的
手順 1	<code>enable</code> 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	<code>configure terminal</code> 例: Router# configure terminal	グローバル 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
<p>手順 3 <code>voice register pool pool-tag</code></p> <p>例: Router(config)# <code>voice register pool 25</code></p>	<p>音声レジスタ プール コンフィギュレーション モードを開始し、Cisco Unified CME の Cisco Unified SIP IP Phone に対して、または Cisco Unified SIP SRST の一連の Cisco Unified SIP IP Phone に対してプール設定を作成します。</p> <ul style="list-style-type: none"> • <i>pool-tag</i>: プールに割り当てる一意の番号。範囲は 1 ~ 100 です。 <p>または</p> <p>音声レジスタ テンプレート コンフィギュレーション モードを開始し、Cisco Unified SIP IP Phone の共通パラメータのテンプレートを定義します。</p> <ul style="list-style-type: none"> • <i>template-tag</i>: テンプレート タグを宣言します。範囲は 1 ~ 10 です。 <p>または</p> <p><code>ephone</code> コンフィギュレーション モードを開始します。</p> <p><i>phone-tag</i>: 設定タスク中にこの <code>ephone</code> を識別する一意のシーケンス番号。<code>ephone</code> の最大数はバージョンやプラットフォームによって異なります。範囲を表示するには、? と入力します。</p>
<p>手順 4 <code>conference-pattern blocked</code></p> <p>例: Router(config-telephony)# <code>conference-pattern blocked</code></p>	<p>Cisco IP Phone から、Cisco IP Phone 以外の電話機の指定された電話番号への電話会議コールが許可されます。</p> <ul style="list-style-type: none"> • <i>conference-pattern blocked</i>: 電話会議は許可されません。
<p>手順 5 <code>exit</code></p> <p>例: Router(config-telephony)# <code>exit</code></p>	<p><code>telephony-service</code> コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。</p>

transfer-pattern blocked

特定の電話機に **transfer-pattern blocked** コマンドが設定されている場合は、その電話機からトランク経由でコールを転送することは一切許可されません。

この機能により、特定の電話機から任意の別の非ローカル番号(あるトランクから別のトランクへの外部コール)へのコール転送はすべて無条件にブロックされます。転送パターンが転送先のダイヤル番号に適合する場合でも、この特定の電話機からのコール転送は許可されません。

表 iii-5 に、特定の設定に関する Cisco Unified SCCP IP Phone と Cisco Unified SIP IP Phone の動作の比較を示します。

表 iii-5 特定の設定に関する Cisco Unified IP Phone の動作

設定	Cisco Unified SCCP IP Phone	Cisco Unified SIP IP Phone
転送パターンが設定されていない。	すべての非ローカル コール転送がブロックされます。	下位互換性のため、すべての非ローカル コール転送が許可されます。
特定の転送パターンが設定されている。	特定の外部エンティティへのコール転送が許可されます。	特定の外部エンティティへのコール転送が許可されます。
transfer-pattern blocked コマンドが設定されている。	すべての非ローカル コール転送がブロックされます。 (注) この設定により、デフォルト(転送パターンが設定されていない状態)に戻ります。	すべての非ローカル コール転送がブロックされます。 (注) この設定により、すべての非ローカル コール転送が無条件でブロックされます。デフォルト(すべての非ローカル コール転送が許可される状態)には戻りません。

conference transfer-pattern

transfer-pattern コマンドと **conference transfer-pattern** コマンドの両方が設定されており、ダイヤル番号が設定されている転送パターンに適合する場合、電話会議が許可されます。ただし、ダイヤル番号が設定されている転送パターンのいずれにも適合しない場合は、電話会議がブロックされます。

HTTPS による Web コンテンツへのセキュアなアクセスのための Cisco Unified IP Phone のプロビジョニングについては、『Cisco Unified Communications Manager Express System Administrator Guide』の「[HTTPS Provisioning for Cisco Unified IP Phones](#)」のセクションを参照してください。

設定例については、『Cisco Unified Communications Manager Administration Guide』の「Configuring HTTPS Support for Cisco Unified CME:Example」のセクションを参照してください。

Cisco Unified SRST バージョン 9.1 の新機能

Cisco Unified SRST 9.1 では、次の新機能がサポートされています。

- [Cisco Unified SIP IP Phone の KEM のサポート \(xxv ページ\)](#)
- [スピードダイヤルサポートの機能強化 \(xxv ページ\)](#)
- [ボイス ハント グループのサポート \(xxvi ページ\)](#)



(注)

VG26nn および VG37nn プラットフォームや Cisco サービス統合型ルータ (ISR) 第 1 世代プラットフォーム (Cisco ISR 1861、2800、および 3800 シリーズ) などの古いルータを使用している場合、これらの新機能を利用するには、Cisco ISR 881、886VA、887VA、888、888E、1861E、2900、3900、および 3900E シリーズ プラットフォームにアップグレードする必要があります。

Cisco Unified SIP IP Phone の KEM のサポート

Cisco Unified 8851/51NR、8861、8961、9951、および 9971 SIP IP Phone では、Cisco Unified SIP SRST 9.1 以降で Cisco Unified IP キー拡張モジュール (KEM) がサポートされています。

Cisco Unified 8851/51NR、8861、8961、9951、および 9971 SIP IP Phone の KEM のサポートについては、『[Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST](#)』を参照してください。

制約事項

- Cisco Unified SRST では、KEM の一括登録はサポートされません。電話機は一括登録要求を送信しませんが、登録には常に User Datagram Protocol (UDP) ポートを使用します。
- KEM は、Cisco Unified 8851/51NR、8861、8961、9951、および 9971 SIP IP Phone 以外の Cisco Unified SCCP IP Phone および Cisco Unified SIP IP Phone ではサポートされません。
- サポート対象の Cisco Unified SIP IP Phone を Cisco Unified SIP SRST で使用している場合、キーに設定した機能はディセーブルになります。
- Cisco Unified 8851/51NR、8861、8961、9951、および 9971 SIP IP Phone の制約事項と制限事項はすべて KEM に適用されます。
- Cisco Unified SIP SRST の機能上の制約事項と制限事項はすべて KEM に適用されます。

音声レジスタ プール コンフィギュレーション モードで **blf-speed-dial**、**number**、および **speed-dial** の各コマンドがどのように変更されているかの詳細については、『[Cisco Unified Communications Manager Express Command Reference](#)』を参照してください。

Cisco Unified IP Phone への KEM のインストールについては、『[Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 7.1 \(3\) \(SIP\)](#)』の「[Installing a Key Expansion Module on the Cisco Unified IP Phone](#)」のセクションを参照してください。

Cisco Unified 8811、8841、8851、8851NR、および 8861 Phone への KEM のインストールについては、『[Cisco IP Phone 8811, 8841, 8851, 8851NR, and 8861 Administration Guide for Cisco Unified Communications Manager](#)』の「[Cisco IP Phone Key Expansion Module](#)」のセクションを参照してください。

スピードダイヤルサポートの機能強化

Cisco Unified SRST 9.1 では、スピードダイヤルサポートの中断を回避するため、一時停止インジケータの「,」（カンマ）が無視されます。

スピードダイヤル一時停止機能 (Cisco Unified Communications Manager または Cisco Unified CM でサポートされている) は Cisco Unified SRST ではサポートされないため、Cisco Unified SRST に登録された Cisco Unified CM および 電話機 (Cisco Unified SCCP IP Phone および Cisco Unified SIP IP Phone) は Cisco Unified SRST モードで下位互換性を保持します。WAN 停止および Cisco Unified CM 障害発生時に電話機が Cisco Unified SRST ルータにフェールオーバーする場合、スピードダイヤル一時停止ボタンを押すと、電話機はスピードダイヤル番号のみを送信します。カンマ一時停止インジケータは無視され、事前設定された FAC、PIN、および DTMF は送信されません。

Cisco Unified Communications Manager でのスピードダイヤルの設定については、『[Cisco Unified Communications Manager Administration Guide](#)』の「[Device setup](#)」の章を参照してください。

ボイス ハント グループのサポート

Cisco Unified SIP SRST 9.1 はボイス ハント グループをサポートしています。ボイス ハント グループにより、1 つの番号(パイロット番号)にコールを発信することで、複数の宛先に接続できます。

ボイス ハント グループには 3 つのタイプがあります。番号が応答するまでパイロット番号に連続したコールが行われた場合について、各タイプでは異なる方法を使用して、最初に呼び出す番号を決定します。

- **パラレル ハント グループ:** 着信コールにより、ハント グループ メンバー リストのすべての番号が同時に呼び出されます。
- **シーケンシャル ハント グループ:** 着信コールにより、ハント グループの定義時にリストに登録された順番(左から右)ですべての番号が呼び出されます。リスト内の最初の番号は、常に、パイロット番号がコールされたときに試行される最初の番号になります。ホップの最大数は、シーケンシャル ハント グループのパラメータとして設定できません。
- **最長アイドルハントグループ:** 着信コールは、ハント グループの定義時に指定されたホップ数の中で、アイドル状態が最も長かった番号に最初につながります。最長のアイドル時間は、電話機が登録された、再登録された、またはオンフックになった最後の時間から求められます。

ePhone ハント グループは Cisco Unified SCCP IP Phone のみをサポートしますが、ボイス ハント グループは Cisco Unified SCCP IP Phone、Cisco Unified SIP IP Phone、または Cisco Unified SCCP IP Phone と Cisco Unified SIP IP Phone の組み合わせをサポートします。

ボイス ハント グループ機能が Cisco Unified SIP SRST ルータで事前設定されている場合は、電話機が Cisco Unified CM から Cisco Unified SIP SRST ルータにフォールバックした後もボイス ハント グループが引き続きサポートされます。

制約事項

- Cisco Unified SRST のボイス ハント グループについては、ハントグループ統計情報がサポートされません。
- あるハント グループの最後の番号を別のハント グループのパイロットとしてネストまたは設定するハント グループはサポートされません。

Cisco Unified SRST バージョン 9.0 の新機能

Cisco Unified SRST 9.0 では、次の新しい Cisco Unified SIP IP Phone がサポートされています。

- Cisco Unified 6901/6911 SIP IP Phone
- Cisco Unified 6921/6941/6945/6961 SIP IP Phone
- Cisco Unified 8941/8945 SIP IP Phone

Cisco Unified SRST 9.0 では、次の新機能がサポートされています。

- [回線ごとの複数コール \(xxvii ページ\)](#)
- [Cisco ATA-187 での音声とファクスのサポート \(xxviii ページ\)](#)

Cisco Unified 6901 および 6911 SIP IP Phone のサポート

Cisco Unified SRST での Cisco Unified 6901 および 6911 SIP IP Phone 関連の機能サポートについては、『[Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST](#)』を参照してください。

Cisco Unified 6921、6941、6945、および 6961 SIP IP Phone のサポート

Cisco Unified SRST での Cisco Unified 6921、6941、6945、および 6961 SIP IP Phone 関連の機能サポートについては、『[Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST](#)』を参照してください。

Cisco Unified 8941 および 8945 SIP IP Phone のサポート

Cisco Unified SRST での Cisco Unified 8941 および 8945 SIP IP Phone 関連の機能サポートについては、『[Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST](#)』を参照してください。

回線ごとの複数コール

Cisco Unified SRST 9.0 は、Cisco Unified 6921、6941、6945、6961 SIP IP Phone、Cisco Unified 8941、8945 SCCP および SIP IP Phone で、回線ごとの複数コール (MCPL) 機能をサポートします。

Cisco Unified SRST 9.0 よりも前は、Cisco Unified 8941 および 8945 SCCP IP Phone の電話番号 (DN) ごとにサポートされているコールの最大数は 2 つに制限されていました。

Cisco Unified SRST 9.0 では、1 回線あたりのコールの最大数の制限が MCPL 機能によって拡大されました。

Cisco Unified SRST 9.0 では、MCPL 機能は Cisco Unified 6921、6941、6945、および 6961 SCCP IP Phone でサポートされていません。これらの電話機で許可されるコールの最大数は 2 つであり、話中のコール転送または話中音がアクティブ化されるまでにこれらの電話機においてオクトラインの電話番号で許可されるコールの最大数は 1 つです。

Cisco Unified 8941/8945 SCCP IP Phone

Cisco Unified SRST 9.0 よりも前は、**max-dn** コマンドと **timeouts busy** コマンドの値は Cisco Unified 8941 および 8945 SCCP IP Phone に関してハードコーディングされていました。

Cisco Unified SRST 9.0 では、**max-dn** コマンドと **timeouts busy** コマンドを **call-manager-fallback** コンフィギュレーション モードで設定できます。ルータでサポート可能な DN の最大数を設定し、二重回線モード、オクトライン モード、または両方のモードを有効にするには、**max-dn** コマンドを使用します。話中の接続先へのコール転送のタイムアウト値を設定するには、**timeouts busy** コマンドを使用します。

設定については、『[コールの最大数の設定](#)』セクション (89 ページ) を参照してください。

Cisco Unified 6921/6941/6945/6961/8941/8945 SIP IP Phone

Cisco Unified SRST 9.0 では、Cisco Unified 6921、6941、6945、6961、8941、および 8945 SIP IP Phone のコールの最大数は電話機によって制御されます。

前提条件

- Cisco Unified SRST 9.0 以降のバージョン。
- 正しいファームウェアがインストールされていること。
 - Cisco Unified 6921、6941、6945、および 6961 SIP IP Phone では 9.2(1) 以降のバージョン。
 - Cisco Unified 8941 および 8945 SIP IP Phone では 9.2(2) 以降のバージョン。

Cisco ATA-187 での音声とファクスのサポート

Cisco ATA-187 は、従来の電話機を IP デバイスに変換する SIP ベースのアナログ電話アダプタです。Cisco ATA-187 は、一方のコネクタに通常のアナログ FXS 電話機またはファクス機器を接続することができます。また、IP 側にあるもう一方のコネクタは、シグナリング用の SIP を使用し、Cisco Unified SIP IP Phone として登録します。

Cisco ATA-187 は、T.38 ファクスリレーおよびファクスパススルーをサポートする Cisco Unified SIP IP Phone として機能し、IP ネットワークを介したファクスのリアルタイム送信を可能にします。ファクスレートは 7.2 ~ 14.4 kbps です。

Cisco Unified SRST での Cisco ATA-187 関連の機能サポートについては、『[Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST](#)』を参照してください。

Cisco ATA-187 の詳細については、『[Cisco ATA 187 Analog Telephone Adaptor Administration Guide for SIP](#)』を参照してください。

Cisco Unified SRST バージョン 8.8 の新機能

Cisco Unified SRST 8.8 では、次の新しい Cisco Unified SCCP IP Phone がサポートされています。

- Cisco Unified 6945 SCCP IP Phone
- Cisco Unified 8941 SCCP IP Phone
- Cisco Unified 8945 SCCP IP Phone

Cisco Unified 6945、8941、および 8945 SCCP IP Phone のサポート

Cisco Unified SRST での Cisco Unified 6945、8941、および 8945 SCCP IP Phone 関連の機能サポートについては、『[Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST](#)』を参照してください。

Cisco Unified 6945 SCCP IP Phone の詳細については、『[Cisco Unified IP Phone 6945 User Guide for Cisco Unified Communications Manager Express Version 8.8 \(SCCP\)](#)』を参照してください。

Cisco Unified 8941/8945 SCCP IP Phone の詳細については、『[Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager Express Version 8.8 \(SCCP\)](#)』を参照してください。

Cisco Unified SRST バージョン 8.0 の新機能

Cisco IP Phone ファームウェア 8.5(3) および Cisco IOS リリース 15.1(1)T 以降、Cisco SRST は、RTP と SRTP の両方のメディア接続が IP Phone のセキュリティ設定に基づいている場合に、UDP、TCP、および TLS 接続を介した SIP シグナリングをサポートします。

Cisco Unified SRST バージョン 7.0/4.3 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 8 つのコールの設定\(オクトライン\) \(87 ページ\)](#)
- [コンサルティブ転送の設定\(120 ページ\)](#)

Cisco Unified SRST バージョン 4.2(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。

- [Enhanced 911 サービス \(69 ページ\)](#) の機能拡張

Cisco Unified SRST バージョン 4.1 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。

- [Enhanced 911 サービス \(69 ページ\)](#)

Cisco Unified SRST バージョン 4.0 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 \(xxix ページ\)](#)
- [Cisco IP Communicator のサポート \(xxx ページ\)](#)
- [SCCP および ATA サポートを使用した FAX パススルー \(xxx ページ\)](#)
- [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 \(SCCP 電話\) \(xxx ページ\)](#)
- [ビデオサポート \(xxxi ページ\)](#)

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 アピランスまたはスピード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 個のライン アピランスまたはスピードダイヤル番号が追加され、合計で 34 個のライン アピランスまたはスピード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でき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。

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、『[Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products](#)』を参照してください。

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の、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 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。

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)、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るようになりました。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。

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 (SCCP 電話)

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、H.323 トポロジの接続が保持されるようになりました。このトポロジでは、Cisco Unified Communications Manager などのエンティティ (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る) によってシグナリングが処理されます。

コールプリザベーションが役立つのは、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サイトにあるため、接続障害が起りやすいような場合です。H.323 VoIP コールプリザベーションの機能拡張は、SIP 電話をサポートしません。

設定については、『[Cisco IOS H.323 Configuration Guide](#)』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、ビデオ パラメータを設定し、Cisco Unified SRST に Cisco Unified CM と同等の機能を保持させることができます。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 CM 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 音声通話の場合と同じです。

詳細については、「[ビデオ パラメータの設定](#)」セクション(267 ページ)を参照してください。

Cisco Unified SRST バージョン 3.4 の新機能

Cisco SRST V3.4 には、次のセクションで説明する新機能が導入されています。

- [Cisco SIP SRST 3.4](#)(xxx1 ページ)

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 サービスとバック ツーバック ユーザーエージェント (B2BUA) 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。これらのサービスは、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 IP Phone 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 電話をサポートできます。Cisco SIP SRST バージョン 3.4 を使用すると、Skinny Client Control Protocol (SCCP) 電話と同じ方法で、SIP 電話から 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 バージョン 3.3 の新機能

Cisco SRST V3.3 には、次のセクションで説明する新機能が導入されています。

- [セキュア SRST](#)(xxx1 ページ)
- [Cisco Unified IP Phone 7970G および Cisco Unified 7971G-GE のサポート](#)(xxx2 ページ)
- [show ephone コマンドの機能拡張](#)(xxx2 ページ)

セキュア 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セキュアな 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 ルータはセキュア 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、セキュアなコール処理機能を再開します。

セキュア 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。認証機能は、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ません。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、「[SCCP および SIP のセキュア SRST の設定](#)」セクション(163 ページ)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、転送、スピードダイヤル、コール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。ファイル認証、デバイス認証、シグナリングの暗号化、メディアの暗号化などのセキュリティ機能もサポートします。

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スピードダイヤル番号のサポート、およびボタンや機能に関する状況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 シリーズのマニュアル](#)のインデックス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、「[Cisco Unified IP Phone 7914 拡張モジュールのサポート](#)」セクション(xliii ページ)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。

Cisco SRST バージョン 3.2 の新機能

Cisco SRST V3.2 には、次のセクション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 (xxxiii ページ)
- `cor` コマンドの機能拡張 (xxxiii ページ)
- `pickup` コマンドの機能拡張 (xxxiii ページ)
- `user-locale` コマンドの機能拡張 (xxxiii ページ)
- Cisco 3845 でサポートされる Cisco Unified IP Phone の台数増加 (xxxiii ページ)
- MOH ライブ フィードのサポート (xxxiv ページ)
- コール プリザベーションのタイムアウトなし (xxxiv ページ)

- [RFC 2833 DTMF リレーのサポート \(xxxiv ページ\)](#)
- [トランスレーション プロファイルのサポート \(xxxiv ページ\)](#)

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コール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。

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 \(All Versions\)](#)』から、**cor** コマンドに関する項目を参照してください。

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ました。このソフト キーを使用すると、SRST の動作中であれば、特定の内線番号に着信した外部のダイヤルイン方式 (DID) コールに対して、別の内線番号から応答することができます。

詳細については、『[Cisco Unified SRST and Cisco Unified SIP SRST Command Reference \(All Versions\)](#)』から、**pickup** コマンドに関する項目を参照してください。

user-locale コマンドの機能拡張

user-locale コマンドは、日本語のカタカナで国コードを表示するように拡張されました。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。

Cisco 3845 でサポートされる Cisco Unified IP Phone の台数増加

Cisco 3845 では、720 台の電話機と最大 960 個の ephone-dn ポート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。

MOH ライブフィードのサポート

Cisco Unified SRST では、**moh-live** コマンドが新しい機能拡張として追加されました。**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、バッテリーを充電するためのサードパーティ製外部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、「[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](#)」セクション (9 ページ) 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 リリース 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、「[Cisco Unified SRST 機能の概要](#)」セクション (1 ページ) を参照してください。

H.323 は、SIP 電話ではサポートされません。

RFC 2833 DTMF リレーのサポート

Cisco Skinny Client Control Protocol (SCCP) 電話 (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 桁表示にのみ対応しています。SCCP 電話からリモートの 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桁情報を送信するには、Cisco SRST 3.2 以降のバージョンで、アウトオブバンド SCCP 桁表示から 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、「[SIP アプリケーションとボイス メールに DTMF リレーを設定する方法](#)」セクション (262 ページ) を参照してください。

Cisco Unity Express システムに接続する SIP ネットワークで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。

トランスレーション プロファイルのサポート

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

- 着信者番号
- 発信者番号
- リダイレクトされた着信者番号

設定の詳細については、「[トランスレーション プロファイルの有効化](#)」セクション (126 ページ) 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。

Cisco SRST バージョン 3.1 の新機能

Cisco SRST V3.1 には、次のセクション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 \(xxxv ページ\)](#)
- [Cisco Unified IP Phone 7936 のサポート \(xxxv ページ\)](#)



(注) Cisco Unified IP Phone については、[Cisco Unified IP Phone 7900 シリーズのマニュアル](#)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 準拠のワイヤレス IP Phone で、Cisco Unified CM 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。Cisco Unified Wireless IP Phone 7920 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、サービス品質 (QoS)、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。

設定は不要です。

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 ベースでハンズ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、ミュート、電話会議など) を提供します。

設定は不要です。

Cisco SRST バージョン 3.0 の新機能

Cisco SRST V3.0 には、次のセクション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 \(xxxvi ページ\)](#)
- [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 \(SCCP 電話\) \(xxxvi ページ\)](#)
- [Cisco Unified IP Phone 用にカスタマイズされたシステム メッセージ \(xxxvi ページ\)](#)
- [二重回線モード \(xxxvii ページ\)](#)
- [E1 R2 シグナリングのサポート \(xxxvii ページ\)](#)
- [欧州の日付形式 \(xxxviii ページ\)](#)
- [二重回線モードのハントストップ \(xxxviii ページ\)](#)
- [フラッシュ ファイルからのマルチキャスト用の保留音 \(xxxviii ページ\)](#)
- [呼び出しタイムアウトのデフォルト \(xxxix ページ\)](#)
- [2 次ダイヤル トーン \(xxxix ページ\)](#)
- [show ephone コマンドの機能拡張 \(xxxix ページ\)](#)
- [電話機の登録に関するシステム ログ メッセージ \(xxxix ページ\)](#)

- 3 者間の G.711 アドホック会議 (xxxix ページ)
- Cisco VG248 Analog Phone Gateway 1.2(1) 以降のバージョンのサポート (xxxix ページ)

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 Unified SRST が Cisco Unified CM 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 (SCCP 電話)

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 コール転送およびブラインド コール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。



(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 リリース 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 リリース 12.2(11)YT 以降のリリースを実行する必要があります。SIP 電話では、この機能はサポートされません。

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、『[Cisco SRST 3.0 で H.450.2 および H.450.3 を使用したコンサルタティブ コールの転送および自動転送の有効化](#)」セクション (133 ページ) 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、これらのディスプレイ 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。

設定については、「[Cisco Unified IP Phone 用にカスタマイズしたシステム メッセージの設定](#)」セクション(83 ページ)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、および電話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、「[二重回線の電話設定](#)」セクション(85 ページ)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、チャネライズド E1 ネットワークに共通の国際的な信号規格です。ただし、R2 に関する単一の信号規格はありません。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、スロバキア共和国を含む)
- 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
- ペルー
- フィリピン
- サウジアラビア
- シンガポール
- 南アフリカ (PanafTel 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 (年-月-日)
- yy-dd-mm (年-日-月)

設定については、「[IP Phone の時計、日付、時刻形式の設定](#)」セクション (80 ページ) 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、「[ダイヤルピア チャネル ハントの設定](#)」セクション (130 ページ) 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保留音

Cisco SRST は、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、「[XML API スキーマの定義](#)」セクション (160 ページ) 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、無応答時のコール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切断コードを返します。このメカニズムにより、転送と切断を監視しない 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、「[呼び出しタイムアウトのデフォルトの設定](#)」セクション(131 ページ)を参照してください。

2 次ダイヤルトーン

2 次ダイヤルトーンは、Cisco SRST を実行している Cisco Unified IP Phone で使用できます。2 次ダイヤルトーンは、ユーザが事前定義 PSTN アクセス プレフィックスをダイヤルしたときに生成されます。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。

2 次ダイヤルトーンを作成するには、secondary dialtone コマンドを使用します。詳細については、「[2 次ダイヤルトーンの設定](#)」セクション(84 ページ)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 で不在転送(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。

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 Unified SRST に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 アドホック会議

Cisco SRST は、G.711 コーディング技術を使用した 3 者間のアドホック会議をサポートしています。会議を使用するには、IP Phone に 1 つ以上のボタンに接続された 2 本以上の回線が必要です。

詳細については、「[3 者間 G.711 アドホック会議の有効化](#)」セクション(159 ページ)を参照してください。

Cisco VG248 Analog Phone Gateway 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 CM 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、FAX 装置、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 CM 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 バージョン 2.1 の新機能

Cisco SRST V2.1 には、次のセクション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 (x1 ページ)
- Cisco SRST の集約 (xli ページ)
- Cisco ATA 186 および ATA 188 のサポート (xli ページ)
- Cisco Unified IP Phone 7902G のサポート (xli ページ)
- Cisco Unified IP Phone 7905G のサポート (xli ページ)
- Cisco Unified IP Phone 7912G のサポート (xli ページ)
- Cisco Unified IP Phone 7914 拡張モジュールのサポート (xlili ページ)
- dialplan-pattern コマンドの機能拡張 (xlili ページ)



(注) Cisco Unified IP Phone については、[Cisco Unified IP Phone 7900 シリーズ](#)の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 Unified SRST が Cisco Unified CM V3.2 の下で動作している場合のみです。

設定については、『[IP Phone の言語表示の設定](#)」セクション (82 ページ) を参照してください。

Cisco SRST の集約

Cisco Unified CM 3.3(2) 以降のバージョン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。コール転送およびコール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 Analog Telephone Adaptor は、通常のアナログ電話を IP ベースのテレフォニー ネットワークで動作できるようにするハンドセット/イーサネット間アダプタです。Cisco ATA は 2 つの音声ポートをサポートし、それぞれに個別の電話番号を割り当てることができます。また、Cisco ATA 188 には RJ-45 10/100BASE-T データポートもあります。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。

Cisco Unified IP Phone 7902G は、リダイヤル、転送、電話会議、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ファンクション 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 経由で電力を得られるようになります。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、ネットワーク可用性が向上します。

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、ピクセルベースの液晶ディスプレイ (LCD) を通してユーザにコールの特徴と機能を案内する 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 経由で電力を得られるようになります。

設定は不要です。

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者の通信ニーズに対応します。4 つの動的なソフト キーを使用して、コールの特徴と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、Cisco Unified IP Phone 7912G 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 経由で電力を得られるようになります。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、ネットワーク可用性が向上します。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

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スピード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スピード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スピード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。

Cisco SRST バージョン 2.02 の新機能

Cisco SRST バージョン 2.02 には、次のセクション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 \(xliv ページ\)](#)
- [電話番号の増加 \(xlv ページ\)](#)
- [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 \(xlvii ページ\)](#)

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ズ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 CM 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 CM 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、ユーザにコールの特徴と機能を案内する 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、Cisco Unified IP Phone 7935 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。設定は不要です。

電話番号の増加

表 iii-6 に、電話番号の増加を示します。

表 iii-6 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	
		送信元	宛先
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 ボイスメールおよび他のボイスメール システムは、Unified SRST と統合できます。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](#)

次の作業

「ネットワークの設定」セクション(53 ページ)に進んでください。

■ 次の作業



Cisco Unified SRST 機能の概要

この章では、Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) とその機能について説明します。また、Cisco Unified IP Phone およびプラットフォームのサポートや、仕様、機能、前提条件、制約事項、および追加の参照資料の入手先についても説明します。

Cisco Unified IP Phone のサポート、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、ならびに Cisco Unified SRST および Cisco Unified SIP SRST のメモリ要件に関する最新情報については、『[Cisco Unified SRST Supported Firmware, Platforms, Memory, and Voice Products](#)』を参照してください。

目次

- [Cisco Unified SCCP SRST \(1 ページ\)](#)
- [Cisco Unified SIP SRST \(9 ページ\)](#)
- [Cisco Unified SRST のライセンス](#)
- [Unified CME と Unified SRST のインターフェイス サポート \(18 ページ\)](#)
- [MGCP ゲートウェイと SRST \(18 ページ\)](#)
- [Cisco Unified IP Phone およびプラットフォームのサポート \(25 ページ\)](#)
- [Unified SRST SIP IP Phone の IPv6 サポート \(19 ページ\)](#)
- [次の作業 \(27 ページ\)](#)
- [その他の関連資料 \(28 ページ\)](#)
- [マニュアルの入手方法およびテクニカル サポート \(30 ページ\)](#)

Cisco Unified SCCP SRST

- [SCCP SRST について \(2 ページ\)](#)
- [Cisco Unified SCCP SRST を設定するための前提条件 \(4 ページ\)](#)
- [Cisco Unified SCCP SRST の設定に関する制約事項 \(7 ページ\)](#)

SCCP SRST について

Cisco Unified SRST は、Cisco Unified CM に、ローカル ネットワーク上の Cisco ルータに接続された Cisco Unified IP Phone のフォールバック サポートを提供します。Cisco Unified SRST を使用すると、ルータはリモートのプライマリ、セカンダリ、またはターシャリ Cisco Unified CM インスタレーションとの接続を失った場合、または WAN 接続がダウンした場合に、Cisco Unified IP Phone にコール処理サポートを提供できます。

Cisco Unified CM は、WAN により Cisco マルチサービス ルータに接続されリモートサイトにある Cisco Unified IP Phone をサポートします。Cisco Unified SRST が導入される前は、ルータと Cisco Unified CM の間の WAN 接続に障害が発生したり、何らかの理由で Cisco Unified CM との接続が失われたりすると、その障害の発生中はネットワーク上の Cisco Unified IP Phone が使用できなくなっていました。Cisco Unified SRST は、Cisco Unified IP Phone のコール処理サポートを Cisco Unified SRST ルータから直接提供することで、この問題を克服し、Cisco Unified IP Phone の継続的なサービス提供(ただし最小限)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) 技術を使用してブランチ オフィスのルータを自動設定することによって、ルータに登録されている Cisco Unified IP Phone のコール処理を提供します。プライマリ Cisco Unified CM との 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 CM に戻ります。

Cisco Unified IP Phone は、プライマリ、セカンダリ、およびターシャリ Cisco Unified CM との接続を失うと、コールの発信および受信に必要なコール処理機能を維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 Unified IP Phone は、[設定 (Settings)] メニューの [ネットワークの設定 (Network Configuration)] エリアで、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。[設定 (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ますが、Cisco Unified CM は最大 3 つのエントリに対応します。セカンダリ Cisco Unified CM がネットワーク上で使用できなくなると、ローカル Cisco Unified SRST ルータの IP アドレスが通常動作時の Cisco Unified CM のスタンバイ接続として保持されます。



(注) Cisco Unified CM 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 Unified IP Phone のみです。ネットワーク上の他の Cisco Unified IP Phone は、プライマリ、セカンダリ、またはターシャリ Cisco Unified CM との接続を再確立するまで、サービスを停止したままになります。

一般に、Cisco Unified CM 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 CM との接続が失われた時点から 10 ~ 20 秒かかります。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 CM のロケーションが登録されている場合のみです。それ以外の場合、電話機はセカンダリ Cisco Unified CM 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、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 CM リストに複数の Cisco Unified CM 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シャリ Cisco Unified CM のリストを処理します。したがって、Cisco Unified 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 CM への接続が試行されるたびに増加します。Cisco Unified CM 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 Unified 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 が有効になると、Cisco Unified IP Phone には、電話機が Cisco Unified CM 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 CM フォールバック モードで動作している場合、たとえば、Cisco Unified IP Phone 7960G および Cisco Unified IP Phone 7940G には「CM フォールバック サービス動作中 (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 フォールバック サービス (CM Fallback Service)」というメッセージが表示されます。Cisco Unified CM 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 CM 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 CM との再接続を定期的に試行します。一般に、Cisco Unified IP Phone がリモートの Cisco Unified CM への再接続を試行するまでのデフォルトの待機時間は 120 秒です。この時間は、Cisco Unified CM で変更できます。該当する Cisco Unified CM のアドミニストレーション ガイドの「デバイス プールの設定」の章を参照してください。手で再起動すると、Cisco Unified IP Phone を Cisco Unified CM にただちに再接続することができます。

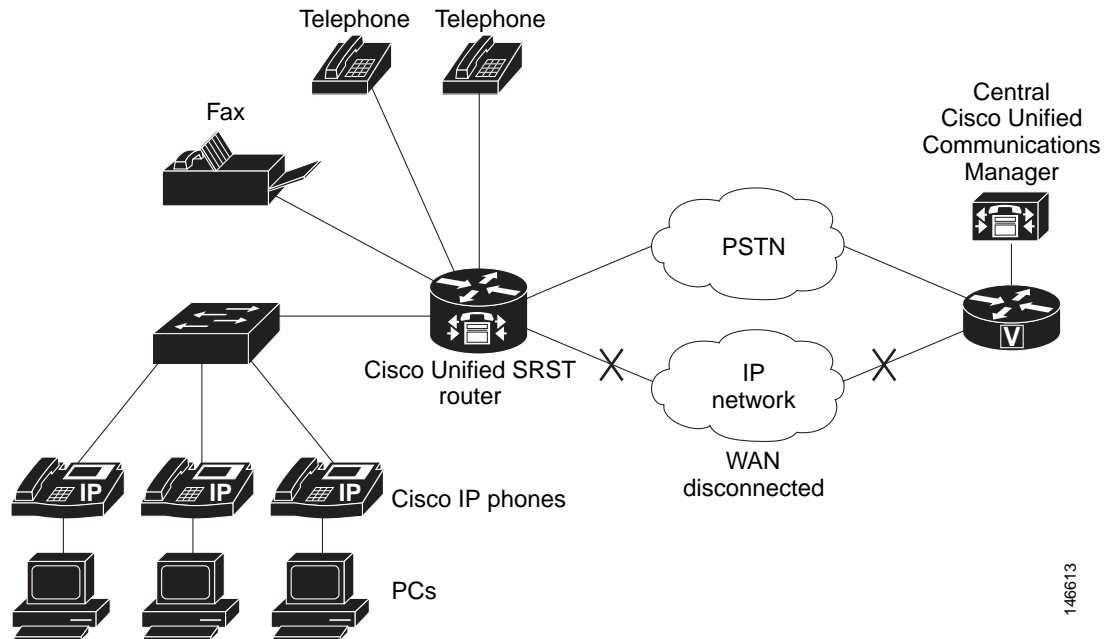
Cisco Unified CM との接続が再確立されると、Cisco Unified IP Phone は、Cisco Unified SRST ルータに対する登録を自動的にキャンセルします。ただし、WAN リンクが不安定な場合、Cisco Unified IP Phone は、Cisco Unified CM と Cisco Unified SRST の間で接続を切り替えることがあります。アクティブ コールを現在受けている場合、Cisco Unified IP Phone では、セントラル オフィスにあるプライマリ Cisco Unified CM との接続を再確立できません。

Cisco Unified SRST は次のコールの組み合わせをサポートしています。

- SCCP 電話から SCCP 電話へ
- SCCP 電話から PSTN/ルータの音声ポートへ
- SCCP 電話から WAN VoIP へ (SIP または H.323 を使用)
- SIP 電話から SIP 電話へ
- SIP 電話から PSTN/ルータの音声ポートへ
- SIP 電話から Skinny Client Control Protocol (SCCP) 電話へ
- SIP 電話から WAN VoIP へ (SIP を使用)

図 1-1 に、Cisco Unified SRST ルータに接続された複数の Cisco Unified IP Phone のあるブランチ オフィスを示します。このルータは、WAN リンクと PSTN の両方への接続を提供します。一般に、Cisco Unified IP Phone は、WAN リンク経由でセントラル オフィスにあるプライマリ Cisco Unified Communications Manager に接続します。WAN 接続がダウンすると、Cisco Unified 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 1-1 SRST モードで動作する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



146613

WAN リンクに障害が発生した場合、デフォルトでは、SCCP SRST の 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 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](#)』ドキュメントを参照してください。

Cisco Unified SCCP SRST を設定するための前提条件

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

- Cisco Unified SCCP SRST 機能を有効にするには SRST 機能ライセンスが必要です。不明な点がある場合は、アカウント担当者までお問い合わせください。Unified SRST のライセンスの詳細については、[Cisco Unified SRST のライセンス \(13 ページ\)](#) を参照してください。
- 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 に移動し、画面上部の [登録 (Register)] をクリックします。

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 Install and Upgrade Guides*』に示されている適切なバージョンのインストール手順に従います。
- 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。「[Cisco Unified SCCP SRST と Cisco Unified Communications Manager の統合](#)」セクション(5 ページ)を参照してください。

Cisco Unified SCCP 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 Unified SRST V3.0 以降のバージョンのインストール](#)(5 ページ)
- [Cisco Unified SRST V2.0 および V2.1 のインストール](#)(5 ページ)
- [Cisco Unified SRST V1.0 のインストール](#)(5 ページ)

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

Cisco Unified SRST V3.0 以降のバージョンのインストール

ご使用のバージョンの Cisco Unified Communications Manager 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。詳細については「[Cisco Unified Communications Manager の互換性](#)」セクション(26 ページ)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、保留音(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、「[XML API スキーマの定義](#)」セクション(160 ページ)を参照してください。MOH の使用を予定している場合は、<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp> の Technical Support Software Download サイトにアクセスし、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 Unified 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てインストールします。

Cisco Unified 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 を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 SCCP SRST と Cisco Unified Communications Manager の統合

Cisco Unified SRST と Cisco Unified Communications Manager 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 アドレスです。

-
- 手順 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、[システム (System)]、[SRST] の順にクリックします。
 - b. [SRST リファレンスの検索と一覧表示 (Find and List SRST References)] ページで、[新規 SRST リファレンスの追加 (Add a New SRST Reference)] をクリックします。
 - c. [SRST リファレンス設定 (SRST Reference Configuration)] ページで、[SRST リファレンス名 (SRST Reference Name)] フィールドに名前を入力し、[IP アドレス (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. [挿入 (Insert)] をクリックします。
- 手順 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、[システム (System)]、[デバイスプール (Device Pool)] の順にクリックします。
 - b. [デバイスプール設定 (Device Pool Configuration)] ページで、目的のデバイスプールのアイコンをクリックします。
 - c. [デバイスプール設定 (Device Pool Configuration)] ページで、[SRST リファレンス (SRST Reference)] フィールドのメニューから SRST リファレンスまたは [デフォルトゲートウェイを使用 (Use Default Gateway)] を選択します。
-

Cisco Unified Communications Manager V3.3 より前のバージョンを使用する場合

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。

-
- 手順 1** Cisco Unified Communications Manager の [電話設定 (Phone Configuration)] ページに移動します。
- a. Cisco Unified Communications Manager の任意のページで、[デバイス (Device)]、[電話 (Phone)] の順にクリックします。
 - b. [電話の検索と一覧表示 (Find and List Phones)] ページで、[検索 (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. [電話設定 (Phone Configuration)] が表示されます。
- 手順 2** [電話設定 (Phone Configuration)] ページで、下部にある [製品固有設定 (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 [有効化 (Enabled)] を選択して、[更新 (Update)] をクリックします。
- 手順 3** ステップ 1 とステップ 2 を繰り返して、次の電話機の [電話設定 (Phone Configuration)] ページに移動し、[Cisco Unified SRST] フィールドのメニューから [有効化 (Enabled)] を選択します。
-

Cisco Unified SCCP SRST の設定に関する制約事項

表 1-1 は、Cisco SCCP SRST バージョン 1.0 から Cisco Unified SCCP 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 1-1 Cisco SCCP SRST の現行バージョンからバージョン1.0 までの制約事項

Cisco Unified SRST のバージョン	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"> • Cisco Unified SRST の Enhanced 911 サービスは、Cisco Emergency Responder とインターフェイスできません。 • Cisco Unified SRST を再起動すると、911 を呼び出した直近の電話についての情報は失われます。 • リモートの IP Phone が Cisco Unified SRST フォールバック モードである場合、Cisco Emergency Responder は、緊急コールの履歴表に行われた更新にアクセスできません。このため、Cisco Unified IP Phone が Cisco Unified Communications Manager に登録し直した後、PSAP がコールバックすると、Cisco Emergency Responder はそれらのコールの履歴を保持しません。その結果、それらのコールは元の 911 発信者にルーティングされません。その代わりに、コールは、対応する ELIN 用に Cisco Emergency Responder に設定されているデフォルトの接続先にルーティングされます。 • Cisco Unified Wireless IP Phone 7920 および 7921 の場合、発信者の位置はシステム管理者によって設定された固定情報によってのみ決定されます。詳細については、「Configuring Enhanced 911 Services」の「Precautions for Mobile Phones」を参照してください。 • 内線番号が 911 の発信者は、緊急応答ロケーション (ERL) ごとに 2 つの緊急ロケーション識別番号 (ELIN) だけに変換できます。 • 複数の目的で ELIN を使用すると、既存の Cisco Unified SRST 機能との予期しない相互作用が発生する場合があります。これらの ELIN の複数の使用方法には、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、または別名ルーティング番号として ELIN を設定することなどがあります。詳細については、「Configuring Enhanced 911 Services」の「Multiple Usages of an ELIN」を参照してください。 • Enhanced 911 サービスの設定が、既存の Cisco Unified SRST 機能と相互作用を及ぼし、予期しない動作となる可能性がある他の方法が多数存在します。Enhanced 911 サービスと既存の Cisco Unified SRST 機能の間の相互作用の詳細については、「Configuring Enhanced 911 Services」の「Interactions with Existing Cisco Unified CME Features」を参照してください。

表 1-1 Cisco SCCP SRST の現行バージョンからバージョン1.0 までの制約事項(続き)

Cisco Unified SRST のバージョン	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"> • Cisco SRST バージョン 1.0 のすべての制約事項。 • サポートされる Cisco Unified IP Phone での発信者 ID 表示: フォールバックモードの SIP 電話には発信者の名前と番号が表示されます。フォールバックモードの SCCP 電話には回線に割り当てられた発信者 ID 番号のみが表示されます。SRST フォールバック中は SCCP 電話の発信者 ID 名設定は保持されません。 • 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"> – Cisco IOS リリース 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 – FXO および FXS ループスタート(アナログ) – FXO および FXS グラウンドスタート(アナログ) – Ear and Mouth (E&M) (アナログ) および DID (アナログ) – FXO および FXS グラウンドスタート シグナリングによる T1 個別線信号方式(CAS) – E&M シグナリングによる T1 CAS – PRI および BRI スイッチの全タイプ • Cisco Unified IP Phone 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"> – ミートミー(MeetMe) – グループ ピックアップ(GPickUp) – パーク (Park) – 会議(Confrn) • Cisco IAD2420 Series Integrated Access Devices (IAD) 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。
バージョン 3.4	12.4(4)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 12.3(4)T	
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 12.2(8)T 12.2(2)XT	
バージョン 1.0	12.2(2)XB 12.2(2)XG 12.1(5)YD	

Cisco Unified SIP SRST

- [SIP SRST について \(9 ページ\)](#)
- [Cisco Unified SIP SRST を設定するための前提条件 \(9 ページ\)](#)
- [Cisco Unified SIP SRST の設定に関する制約事項 \(10 ページ\)](#)

SIP SRST について

このガイドでは、SIP ネットワーク関連の Cisco Unified SRST 機能について説明します。Cisco Unified SIP SRST は、基本的なレジストラ サービスとリダイレクト サーバまたはバックツールバック ユーザエージェント (B2BUA) サービスを提供することにより、外部の SIP プロキシサーバへのバックアップを行います。これらのサービスは、WAN 接続が停止して SIP IP Phone がブライマリ SIP プロキシと通信できなくなった場合に、その SIP IP Phone によって使用されます。

Cisco Unified SIP SRST 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 電話をサポートできます。Cisco Unified SIP SRST を使用すると、SCCP 電話と同じ方法で、SIP 電話から SIP ネットワークを介してコールを発信できます。

Cisco Unified SIP SRST は次のコールの組み合わせをサポートしています。

- SIP 電話から SIP 電話へ
- SIP 電話から PSTN/ルータの音声ポートへ
- SIP 電話から Skinny Client Control Protocol (SCCP) 電話へ
- SIP 電話から WAN VoIP へ (SIP を使用)

SIP プロキシ、レジストラ、および B2BUA サーバは SIP VoIP ネットワークの主要コンポーネントです。これらのサーバは、通常、VoIP ネットワークのコアに配置されます。VoIP ネットワークのエッジのリモートサイトにある SIP 電話がネットワーク コアとの接続を失う (WAN 停止のため) と、それらの電話機でコールの発信または受信ができなくなる場合があります。SIP PSTN ゲートウェイの Cisco Unified SIP SRST 機能は、WAN 停止時における SIP ベース IP Phone のサービスの信頼性を提供します。Cisco Unified SIP SRST により、SIP IP Phone は、PSTN との間でのコールの発信および受信や、他の SIP IP Phone との間でのコールの発信および受信を継続できます。

SRST モードで動作するリモートのセントラル Cisco Unified CM に接続されたブランチ オフィスの Cisco Unified IP Phone の例については、[図 1-1](#) を参照してください。



(注)

Cisco Unity Express (CUE) とセキュアな SIP SRST とのインターワーキングはサポートされません。

Cisco Unified SIP SRST を設定するための前提条件

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

- Cisco Unified SIP SRST 機能を有効にするには SRST 機能ライセンスが必要です。不明な点がある場合は、アカウント担当者までお問い合わせください。Unified SRST のライセンスの詳細については、[Cisco Unified SRST のライセンス \(13 ページ\)](#) を参照してください。

Cisco Unified SIP SRST の設定に関する制約事項

表 1-2 は、Cisco SIP SRST バージョン 3.0 から Cisco Unified SIP 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 1-2 Cisco SIP SRST の現行バージョンからバージョン 3.0 までの制約事項

Cisco Unified SRST のバージョン	Cisco IOS リリース	制約事項
バージョン 8.0	15.1(1)T	<ul style="list-style-type: none"> SIP 電話は Cisco Unified CM で認証済みデバイス セキュリティ モードに設定できません。Cisco Unified CM は、シグナリングに NULL-SHA 暗号を使用する TLS 接続によって、電話機の整合性と認証を保証します。このような認証済みモードの SIP 電話が Cisco Unified SRST デバイスにフェールオーバーする場合、Cisco Unified CM および SRST デバイスがセキュアな SIP SRST をサポートするように設定されているときは、デバイスが TLS/TCP ではなく TCP を使用して登録されるため、SIP 電話が Cisco Unified CM にフェールバックするまで認証済みモードは無効になります。

表 1-2 Cisco SIP SRST の現行バージョンからバージョン3.0 までの制約事項(続き)

Cisco Unified SRST のバージョン	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"> • Cisco Unified SRST は、BLF スピードダイヤル通知、不在転送の同期、ダイヤルプラン、ディレクトリ サービス、または保留音(MOH)をサポートしていません。 • SIP 電話ロード 8.0 より前の SIP 電話では、Cisco Unified Communications Manager と Cisco Unified SRST の両方へのデュアル登録が同時に保持されていました。SIP 電話ロード 8.0 以降のバージョンの SIP 電話では、Cisco Unified Communications Manager への登録がアクティブのときは、キープアライブを使用して Cisco Unified SRST との接続が保持されます。SIP 電話は 2 分ごとにキープアライブ メッセージを Cisco Unified SRST に送信します。Cisco Unified SRST は、このキープアライブに 404 メッセージで応答します。このプロセスは、Cisco Unified SRST へのフォールバックが発生するまで繰り返されます。フォールバックの後は、SIP 電話は 2 分ごとにキープアライブ メッセージを Cisco Unified Communications Manager に送信し、その間、SIP 電話は Cisco Unified SRST に登録されます。Cisco Unified SRST は、8.0 より前の SIP 電話ロードのデュアル登録を引き続きサポートします。 • Cisco Unified SRST の Enhanced 911 サービスは、Cisco Emergency Responder とインターフェイスできません。 • Cisco Unified SRST を再起動すると、911 を呼び出した直近の電話についての情報は失われます。 • リモートの IP Phone が Cisco Unified SRST フォールバック モードである場合、Cisco Emergency Responder は、緊急コールの履歴表に行われた更新にアクセスできません。このため、Cisco Unified IP Phone が Cisco Unified Communications Manager に登録し直した後、PSAP がコールバックすると、Cisco Emergency Responder はそれらのコールの履歴を保持しません。その結果、それらのコールは元の 911 発信者にルーティングされません。その代わりに、コールは、対応する ELIN 用に Cisco Emergency Responder 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。 • Cisco Unified Wireless 7920 および 7921 IP Phone の場合、発信者の位置はシステム管理者によって設定された固定情報によってのみ決定されます。詳細については、「Configuring Enhanced 911 Services」の「Precautions for Mobile Phones」を参照してください。 • 内線番号が 911 の発信者は、緊急応答ロケーション(ERL)ごとに 2 つの緊急ロケーション識別番号(ELIN)だけに変換できます。 • 複数の目的で ELIN を使用すると、既存の Cisco Unified SRST 機能との予期しない相互作用が発生する場合があります。これらの ELIN の複数の使用方法には、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、または別名ルーティング番号として ELIN を設定することなどがあります。詳細については、「Configuring Enhanced 911 Services」の「Multiple Usages of an ELIN」を参照してください。 • Enhanced 911 サービスの設定が、既存の Cisco Unified SRST 機能と相互作用を及ぼし、予期しない動作となる可能性がある他の方法が多数存在します。Enhanced 911 サービスと既存の Cisco Unified SRST 機能の間の相互作用の詳細については、「Configuring Enhanced 911 Services」の「Interactions with Existing Cisco Unified CME Features」を参照してください。

表 1-2 Cisco SIP SRST の現行バージョンからバージョン3.0 までの制約事項(続き)

Cisco Unified SRST のバージョン	Cisco IOS リリース	制約事項
バージョン 4.0	12.4(4)XC	未サポート
バージョン 3.4	12.4(4)T	<ul style="list-style-type: none"> SIP 電話機から呼び出されたコール保留に対しては、MOH はサポートされていません。SIP 電話機によって保留中にされた場合、発信者は何も聞こえません。
バージョン 3.2	12.3(11)T	<ul style="list-style-type: none"> Cisco IOS リリース 12.4(4)T の時点では、ブリッジされたコール アピランス、FindMe、着信コールスクリーニング、ページング、SIP プレゼンス、コールパーク、コールピックアップ、および SIP ロケーションはサポートされていません。
バージョン 3.1	12.3(7)T	<ul style="list-style-type: none"> SIP-NAT はサポートされていません。
バージョン 3.0	12.2(15)ZJ 12.3(4)T	<ul style="list-style-type: none"> Cisco Unity Express はサポートされていません。 トランスコーディングはサポートされていません。 <p>電話機能</p> <ul style="list-style-type: none"> Cisco ATA、Cisco IP Phone 7912、および Cisco Unified IP Phone 7905G (1.0(2)ビルド) でコール ウェイティングを使用するには、G.711 コーデックによって着信コール レッグを設定する必要があります。 <p> (注) Cisco Unified IP Phone 7905G、Cisco Unified IP Phone 7912G、および Cisco Analog Telephone Adapter (ATA) 186 は、デュアル登録に対応していません。このため、それらは、Cisco Unified SIP SRST でサポートされておらず、機能が制限されます。</p> <p>一般</p> <ul style="list-style-type: none"> コール詳細レコード(CDR)は標準 IOS RADIUS サポートによってのみサポートされ、他の方法ではサポートされません。 すべてのコールが同じコーデック (G.729r8 または G.711) を使用する必要があります。 転送されたコールをもう一度転送することはできません。 URL ダイヤルはサポートされていません。番号ダイヤルのみがサポートされています。 Cisco Unified SIP SRST によって提供される SIP レジストラ機能では、セキュリティまたは認証サービスは提供されません。 プライマリとバックアップの両方の SIP プロキシまたはレジストラによるデュアル同時登録をサポートしていない SIP IP Phone は、WAN 停止時に Cisco Unified SIP SRST ゲートウェイからの着信コールを受信できない可能性があります。これらの電話機は、バックアップ プロキシまたはレジストラ (SIP SRST ゲートウェイ) への登録のフォールバックを開始する前に、プライマリ SIP プロキシまたはレジストラが到達不能になっていることを検出するために時間がかかる場合があります。 「SIP 電話から SIP トランクへ」をサポートするには、「参照および 302/300 リダイレクション」が SIP トランク (バージョン 3.0) によってサポートされる必要があります。

Cisco Unified SRST のライセンス

Unified SRST の使用について権限付与する Cisco Unified SRST ライセンスを購入する必要があります。次のライセンスを購入できます。

- Cisco Unified SRST の無期限ライセンスまたは
- Collaborative Professional Suite ライセンス
- Cisco Smart License

Cisco Unified SRST の無期限ライセンス

Cisco Unified SRST の無期限ライセンスを購入すると、製品の出荷時に無期限ライセンスがデバイスにインストールされます。無期限ライセンスは期限切れになることがなく、すべての IOS リリースにわたり、デバイスのライフタイム中は特定の機能セットにアクセスできます。Cisco Unified SRST の無期限ライセンスを購入する場合は、評価使用権および使用権 (RTU) ライセンスプロセスを経ることなく機能を使用できます。既存のデバイスの CME-SRST ライセンスを購入する場合は、機能を使用するための RTU ライセンス プロセスを経る必要があります。ライセンスを購入するための既存のプロセスに変更はありません。

Cisco Unified SRST の無期限ライセンスは XML `cme-locked3` ファイルの形式で提供されます。この XML ファイルを取得し、デバイスのフラッシュ メモリにロードする必要があります。コマンドプロンプトから無期限ライセンスをインストールするには、`license install flash0:cme-locked3` コマンドを使用します。ここで、`cme-locked3` はライセンスの XML ファイルです。

Collaborative Professional Suite ライセンス

Collaboration Professional は新しいライセンススイートです。Collaboration Professional Suite は無期限ライセンスまたは RTU ライセンスとして購入できます。

Collaboration Professional Suite 無期限ライセンス: この Collaboration Professional Suite ライセンスを購入する場合は、デフォルトで、Cisco Unified SRST のライセンスが Collaboration Professional Suite の一部として提供されます。Cisco Unified SRST ライセンスを個別にインストールしてアクティブにする必要はありません。Collaboration Professional Suite 無期限ライセンスは XML ファイルの形式で提供されます。この XML ファイルを取得し、デバイスのフラッシュメモリにロードする必要があります。コマンドプロンプトから無期限ライセンスをインストールするには、`license install flash:lic_name` コマンドを使用します。

Collaboration Professional Suite RTU ライセンス: Collaboration Professional Suite RTU ライセンスを購入する場合は、評価使用権プロセスを経る必要がありません。ただし、Cisco Unified SRST 機能を使用するには、RTU ライセンス プロセスを経る必要があります。コマンドプロンプトから Collaborative Professional Suite RTU ライセンスをインストールするには、`license install flash0:colla_pro` コマンドを使用します。ライセンスを有効にするには、`license boot module c2951 technology-package collabProSuitek9` コマンドを使用します。

また、次の作業も行う必要があります。

- 適切な Cisco Unified SRST バージョンを選択します。各 SRST バージョンは、IP Phone、メモリ要件、機能、および DN の特定のセットをサポートしています。「プラットフォームとメモリのサポート」セクション(26 ページ)および「Cisco Unified SCCP SRST の設定に関する制約事項」セクション(7 ページ)を参照してください。
- 適切な電話機ロードを選択します。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ています。最新の電話機ロードについては、『Cisco Unified SRST Supported Firmware, Platforms, Memory, and Voice Products』を参照してください。

Cisco Unified Communications Manager がすでにインストールされている場合は、その Cisco Unified Communications Manager がご使用の Cisco Unified SRST リリースと互換性のあるバージョンであることを確認します。「Cisco Unified Communications Manager の互換性」セクション(26 ページ)

Cisco Smart License

リリース 12.1 以降、Unified SRST は既存の CSL ライセンス モデルとは別に、スマート ライセンシングをサポートします。スマート ライセンシングは、Cisco 4000 シリーズ サービス統合型ルータでのみサポートされます。ルータで利用可能な技術パッケージに応じて、UCK9 やセキュリティなどのライセンスは、スマート ライセンシングを使用してサポートされます。

スマート ソフトウェア ライセンシングは、ライセンス所有権や利用を把握できるようにするための、シスコの新しいライセンシング モデルです。スマート ライセンスは、クラウドベースの導入モデルである Cisco Smart Software Manager (CSSM)、またはオンプレミス ソフトウェアであるスマート ソフトウェア マネージャ サテライトで管理できます。Unified SRST は CSSM とサテライトの両方でサポートされます。CSSM に存在するカスタマー スマート アカウントへのアクセスは、有効なシスコ クレデンシャルを使用して認証されます。Unified SRST のスマート ライセンシング サポートを使用して、デバイスを CSSM またはシスコ スマート ソフトウェア マネージャ サテライトに登録できます。ライセンスには [Cisco Software Central](#) でアクセスできます。

Unified SRST でライセンス利用をレポートするには、CSSM またはシスコ スマート ソフトウェア マネージャ サテライトに登録する必要があります。スマート アカウント内でトークン ID を生成し、それを基礎プラットフォームの Cisco 4000 シリーズ サービス統合型ルータにペーストすることで、Unified SRST をバーチャル アカウントに対して登録できます。トークンは、生成されたら、ネットワークで他の多くの製品インスタンスに登録するために使用できます。

Unified SRST ルータで、Call Home 機能が無効になっていないことを確認する必要があります。また、スマート ライセンシングは、CLI コマンド **license smart enable** を使用してルータで有効にする必要があります。Smart Licensing を無効にするには、コマンドの **no** 形式を使用します。

ルータでのスマート ライセンシングの設定の詳細については、『[Cisco 4000 Series ISRs Software Configuration Guide](#)』を参照してください。デバイスに対する Call Home の設定の詳細については、『[Call Home の設定](#) (16 ページ)』を参照してください。スマート ライセンシングを有効にすると、ルータは 90 日間の評価期間に入り、ルータを CSSM またはシスコ スマート ソフトウェア マネージャ サテライトに登録するまでその期間は持続します。

ルータはトークン ID を使用して CSSM またはシスコ スマート ソフトウェア マネージャ サテライトに登録できます。デバイス (Unified SRST ルータ) を CSSM またはシスコ スマート ソフトウェア マネージャ サテライトに登録するには、CLI コマンド **license smart register idtoken** を使用します。デバイスの CSSM への登録については、『[Device Registration, Software Activation Configuration Guide, Cisco IOS Release 15M&T](#)』を参照してください。

登録が成功したら、Unified SRST は登録済みステータスになります。登録プロセスの一環として、ルータは承認要求を送信し、SIP SRST の場合は **max-pool**、SCCP SRST の場合は **max-ephone** によって定義された電話機エンドポイントの数を指示します。スマート アカウントのライセンスに基づいて、CSSM またはシスコ スマート ソフトウェア マネージャ サテライトは、承認済み (使用しているのが CSSM またはシスコ スマート ソフトウェア マネージャ サテライトで準備されたライセンス数以下である) またはコンプライアンス違反 (使用しているのが所持ライセンス数を超えている) などの定義済みステータスのいずれかで応答します。

Unified SRST のライセンス制限は、Unified SRST ルータに定義された最大プラットフォーム限度によって制限されます (**max-pool** および **max-ephone** の下で設定された電話機の累積数)。したがって、ライセンス使用数は、**max-pool** と **max-ephone** の下で設定された電話機の累積数が、定義されているプラットフォーム限度を超えている場合でも、Unified SRST ルータに設定されたプラットフォーム限度を超えることはできません。Unified SRST に対して定義されているプラットフォーム限度の詳細については、『[Cisco Unified SRST/E-SRST 12.1 Supported Firmware, Platforms, Memory, and Voice Products](#)』を参照してください。

CSSM またはスマート ソフトウェア マネージャ サテライトは、そのユーザ インターフェイス (UI) でプラットフォームによって送信されたライセンス使用数を報告し、スマート アカウントのバーチャル アカウントで利用可能なライセンス数からその数を減算します。Unified SRST は、Unified SRST 上で設定されている電話機を検証するために、1 ライセンス資格のみをサポートします。

SRST_EP: このライセンス タイプは、Unified SRST で設定されているすべての電話機をサポートします。



(注) SRST_EP ライセンス数は、電話機が登録されているかどうかに関係なく、Unified SRST で設定されている ephone とプールの両方の合計電話機数を反映します。

ライセンス利用が変更される時点または 30 日ごとに、Unified SRST は承認要求を送信し、CSSM またはシスコ スマート ソフトウェア マネージャ サテライトに引き続き利用可能であり通信していることを示します。登録時に Unified SRST を識別するために発行される ID 証明書は 1 年間有効であり、6 ヶ月ごとに自動的に更新されます。



(注) ルータが 90 日間、CSSM またはシスコ スマート ソフトウェア マネージャ サテライトと通信しない場合、ライセンス認証は有効期限切れになります。ライセンス認証の有効期限が切れると、Unified SRST で登録されたデバイスのステータスは、コンプライアンス違反に変更されます。

ライセンス数は、ルータ間で設定されている電話機の数で評価されます。[CSSM ライセンス (CSSM Licenses)] ページには、使用ライセンス合計数、特定タイプのライセンスで利用可能なライセンスの合計数 ([数量 (Quantity)])、現在使用されているライセンスの数 ([使用中 (In Use)])、未使用または超過使用ライセンスの数 ([余剰/不足 (Surplus/Shortage)]) が反映されます。十分な数のシスコ スマート ライセンスを持っていない場合には、コンプライアンス違反状態になります。

たとえば、50 の SRST_EP ライセンスがある CSSM でのスマート アカウントについて考えてみましょう。20 の電話機が設定された登録済みの Unified SRST がある場合、CSSM ライセンス ページでは、[数量 (Quantity)] は 50、[使用中 (In Use)] は 20、および [余剰 (Surplus)] は 30 と反映されます。Smart Software Manager の詳細については、『[Cisco Smart Software Manager User Guide](#)』を参照してください。

CSL とシスコ スマート ライセンスの切り替えの詳細については、[ライセンス モード \(17 ページ\)](#) を参照してください。

Unified SRST スマート ライセンスのライセンス資格は、ルータでは次のように表示されます。

```
Router# show license summary
Smart Licensing is ENABLED

Registration:
Status: REGISTERED
Smart Account: ABC
Virtual Account: XYZ
Export-Controlled Functionality: Not Allowed
Last Renewal Attempt: None
Next Renewal Attempt: Jun 07 12:08:10 2017 UTC

License Authorization:
Status: AUTHORIZED
Last Communication Attempt: SUCCESS
Next Communication Attempt: Apr 13 07:11:48 2017 UTC

License Usage:

License                Entitlement tag                Count  Status
-----
regid.2014-12.com.ci... (ISR_4351_UnifiedCommun..)  1      AUTHORIZED
regid.2016-10.com.ci... (SRST_EP)                    4      AUTHORIZED
```

Call Home の設定

HTTP プロキシ要求に対して Call Home 宛先アドレスとプロキシ サーバの詳細を設定するには、次の手順に従います。

前提条件

- シスコ スマート ソフトウェア ライセンシングが有効である必要があります。

手順の概要

- configure terminal**
- call-home destination address *http url***
- call-home http-proxy *proxy_address port port number***
- end**

手順の詳細

	コマンドまたはアクション	目的
手順 1	<code>configure terminal</code> 例: Router# <code>configure terminal</code>	設定モードを開始します。
手順 2	<code>call-home destination address http url</code> 例: Router(config)# <code>call-home destination address http http://10.22.183.117:8080/ddce/services/DDCEService</code>	(任意) ライセンス要求を含む、Call Home メッセージの宛先 URL を定義します。宛先 URL は、トランスポートゲートウェイまたは CSSM サテライトの URL にできます。 シスコ スマート ライセンシング 運用サーバの URL は、デフォルトで設定されます。
手順 3	<code>call-home http-proxy proxy_address port port number</code> 例: Router(config)# <code>call-home http-proxy 7.7.7.7 port 3218</code>	(任意) HTTP 要求のプロキシサーバを指定します。
手順 4	<code>end</code> 例: Router(config)# <code>end</code>	特権 EXEC モードに戻ります。

ライセンス モード

Unified SRST 12.1 以降から、CSL とスマート ライセンシングの両方のモードがサポートされています。つまり、カスタマーはスマート ライセンシングを有効にしないで CSL を続行できます。または、カスタマーはスマート ライセンシングを有効にしてから後で CSL に戻る場合、**no license smart enable** コマンドでスマート ライセンシングを無効にできます。スマート ライセンシング モードから CSL に切り替える場合には、エンド ユーザ ライセンス契約 (EULA) が署名されていることを確認する必要があります。CSL は、EULA が署名されていない限り、サポートされません。EULA を設定するには、CLI コマンド **license accept end user agreement** をグローバル設定モードで使用します。

Unified SRST で登録された電話機に対して発行されているライセンスのステータスを確認するには、**show license** コマンドを使用できます。

```
Router#show license ?
all          Show license all information
status      Show license status information
summary     Show license summary
tech        Show license tech support information
udi         Show license udi information
usage       Show license usage information
```

制限事項

- Unified SRST ライセンスについては、Collaboration Professional Suite パッケージがインストールされていない場合、UCK9 技術パッケージを使用できる必要があります。

ライセンスを購入するには、<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key> にアクセスします。cme-srst 機能ライセンスをアクティブにするには、『[Activating CME-SRST Feature License](#)』を参照してください。

Unified CME と Unified SRST のインターフェイス サポート

Unified CME ルータと Unified SRST ルータには、シグナリングとデータ パケット転送に使用される複数のインターフェイスがあります。Cisco ルータで利用可能な 2 つのタイプのインターフェイスには、物理インターフェイスと仮想インターフェイスがあります。ルータで利用可能な物理インターフェイスのタイプは、そのインターフェイス プロセッサまたはポート アダプタによって異なります。仮想インターフェイスは、ユーザが Cisco IOS コマンドを使用してネットワークワーキング デバイスのメモリに作成したソフトウェア ベースのインターフェイスです。接続用に仮想インターフェイスを設定する必要がある場合、Unified CME と Unified SRST のループバック インターフェイスを使用できます。

次のインターフェイスは、Unified CME と Unified SRST でサポートされます。

- ギガビットイーサネット インターフェイス (IEEE 802.3z) (**interface gigabitethernet**)
- ループバック インターフェイス (**interface loopback**)
- ファストイーサネット インターフェイス (**interface fastethernet**)

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 リリース 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 より前の 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、『[MGCP ゲートウェイでの Cisco Unified SRST のイネーブル化](#)」セクション (54 ページ) のセクションを参照してください。



(注)

上記のコマンドは、両方のコマンドが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。

Unified SRST SIP IP Phone の IPv6 サポート

インターネットプロトコルバージョン 6 (IPv6) は、インターネットプロトコル (IP) の最新バージョンです。IPv6 は、デジタルネットワークを介したデータ、音声、およびビデオのトラフィックの交換にパケットを使用します。IPv6 では、ネットワーク アドレス ビット数が、IPv4 の 32 ビットから 128 ビットに増やされています。Unified SRST リリース 12.0 以降、Unified SRST は SIP の IP Phone 用の IPv6 プロトコルをサポートしています。

Unified SRST の IPv6 サポートにより、デュアルスタック (IPv4 および IPv6) 環境でネットワークが透過的に動作し、ネットワークに接続された SIP IP 電話機に追加の IP アドレス空間を提供します。デュアルスタック設定でない場合には、デュアルスタック モードに変更する前に、CLI コマンド **call service stop** を **voice service voip** 設定モードの下で設定します。デュアルスタックモードへの切り替えの例については、『[SIP IP Phone の IPv6 プールの設定例 \(24 ページ\)](#)』を参照してください。

Cisco IP Phone 7800 シリーズと 8800 シリーズは、Unified SRST の IPv6 でサポートされます。

IPv6 送信元アドレス向けに SIP IP Phone を設定する手順については、『[SIP IP Phone の IPv6 プールの設定 \(20 ページ\)](#)』を参照してください。

Unified SRST の IPv6 サポートの設定例については、『[SIP IP Phone の IPv6 プールの設定例 \(24 ページ\)](#)』を参照してください。

IPv6 の展開の詳細については、『[IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.0](#)』を参照してください。

Unified SRST SIP IP Phone での IPv6 の機能サポート

次の基本的な機能は、IPv6 WAN シナリオでサポートされます。

- Unified SRST がデュアルスタック **no anat** モードの場合の、基本 SIP 回線間 (IPv4 または IPv6) のコール。

次の補足サービスは、Unified SRST IP 電話で IPv6 の一部としてサポートされます。

- 保留/復帰
- コール転送 (コール受信時に転送)
- コール転送 (コール受信後に転送)
- 3 ウェイ会議 (BIB 会議のみ)
- 補足サービス機能がある T1/E1 トランクへの回線および回線へのトランク
- T.38 ファックス リレーとファックス パススルーの両方に対する、PSTN とやり取りするファックス (IPv4 ATA から ISDN T1/E1)

制限事項

以下に示すのは、Unified SRST での IPv6 サポートの既知の制約事項です。

- SIP トランクは、IPv6 導入の Unified SRST ではサポートされません。PSTN コールは、T1/E1 トランクを介してのみサポートされます。

- SCCP IP Phone は、Unified SRST の IPv6 の導入ではサポートされません。
- SIP Phone は IPv4 または IPv6 のいずれかの専用モードにできます (**no anat**)。
- トランスコーディングとトランスレーティングはサポートされていません。
- H.323 トランクはサポートされていません。
- セキュア SIP 回線またはトランクはサポートされていません。

SIP IP Phone の IPv6 プールの設定

はじめる前に

- Unified SRST 12.0 以降のバージョン。
- IPv6 オプションは、プロトコルモードが **sip-ua** 設定モードまたは IPv6 の下で設定されたデュアルスタックである場合にのみ表示されます。
- Cisco Unified SRST ライセンスは、IPv6 機能をサポートするために、Unified SRST ゲートウェイとして機能するゲートウェイ向けに設定する必要があります。ライセンスの詳細については、[Cisco Unified SRST のライセンス \(13 ページ\)](#) を参照してください。
- Cisco Unified Communications Manager (Unified Communications Manager) は、Unified SRST の IPv6 アドレスを使用してプロビジョニングされます。Unified Communications Manager 上での Unified SRST の設定については、『Cisco Unified Communications Manager Administration Guide』の「[Survivable Remote Site Telephony Configuration](#)」のセクションを参照してください。

手順の概要

5. **enable**
6. **configure terminal**
7. **ipv6 unicast-routing**
8. **voice service voip**
9. **sip**
10. **no anat**
11. **call service stop**
12. **exit**
13. **exit**
14. **sip-ua**
15. **protocol mode {ipv4 | ipv6 | dual-stack [preference {ipv4 | ipv6}]}**
16. **exit**
17. **voice service {voip}**
18. **sip**
19. **no call service stop**
20. **exit**
21. **voice register global**

22. **default mode**
23. **max-dn** *max-directory-numbers*
24. **max-pool** *max-voice-register-pools*
25. **exit**
26. **voice register pool** *pool-tag*
27. **id** { **network** *address mask mask* | **ip address** *mask mask* | **mac** *address* }
28. **end**

手順の詳細

	コマンドまたはアクション	目的
手順 1	enable 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	configure terminal 例: Router #configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	ipv6 unicast-routing 例: Router(config)# ipv6 unicast-routing	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
手順 4	voice service voip 例: Router (config)# voice service voip	音声サービス コンフィギュレーション モードを開始し、音声カプセル化タイプを指定します。 • voip: Voice over IP (VoIP) パラメータを指定します。
手順 5	sip 例: Router(config-voi-serv)# sip	SIP コンフィギュレーション モードを開始します。
手順 6	no anat 例: Router(config-serv-sip)# no anat	SIP トランク上で代替ネットワーク アドレス タイプ (ANAT) を無効にします。
手順 7	call service stop 例: Router(config-serv-sip)# call service stop	SIP コール サービスをシャットダウンします。

	コマンドまたはアクション	目的
手順 8	<code>exit</code> 例: Router(config-serv-sip)# exit	SIP 設定モードを終了します。
手順 9	<code>exit</code> 例: Router(config-voi-sip)# exit	voice service voip コンフィギュレーション モードを終了します。
手順 10	<code>sip-ua</code> 例: Router(config)# sip-ua	SIP ユーザ エージェント コンフィギュレーション モードを開始します。
手順 11	<code>protocol mode {ipv4 ipv6 dual-stack [preference {ipv4 ipv6}]}</code> 例: Router(config-sip-ua)# protocol mode dual-stack preference ipv6	電話機で、IPv6 音声ゲートウェイ上の電話機と対話できます。電話機で IPv4 アドレス、IPv6 アドレス、またはデュアルスタック モードを設定できます。 <ul style="list-style-type: none">• <code>ipv4</code>: プロトコル モードを IPv4 アドレスに設定できます。• <code>ipv6</code>: プロトコル モードを IPv6 アドレスに設定できます。• <code>dual-stack</code>: プロトコル モードを IPv4 アドレスと IPv6 アドレスの両方に設定できます。• <code>preference</code>: プロトコル モードがデュアルスタックの場合に、優先する IP アドレス ファミリを選択できます。
手順 12	<code>exit</code> 例: Router(config-sip-ua)# exit	SIP 設定モードを終了します。
手順 13	<code>voice service {voip}</code> 例: Router (config)# voice service voip	音声サービス コンフィギュレーション モードを開始し、音声カプセル化タイプを指定します。 <ul style="list-style-type: none">• <code>voip</code>: Voice over IP (VoIP) パラメータを指定します。
手順 14	<code>sip</code> 例: Router(config-voi-serv)# sip	SIP コンフィギュレーション モードを開始します。
手順 15	<code>no call service stop</code> 例: Router(config-serv-sip)# call service stop	SIP コール サービスを有効化します。

	コマンドまたはアクション	目的
手順 16	<code>exit</code> 例: <code>Router(config-serv-sip)# exit</code>	SIP 設定モードを終了します。
手順 17	<code>voice register global</code> 例: <code>Router(config)# voice register global</code>	音声レジスタ グローバル コンフィギュレーション モードを開始して、Cisco Unified CME でサポートされるすべての SIP 電話機に対してパラメータを設定します。
手順 18	<code>default mode</code> 例: <code>Router(config-register-global)# default mode</code>	Unified SRST で SIP 電話機をプロビジョニングするためのモードをイネーブルにします。デフォルトのモードは、Unified SRST 自体です。
手順 19	<code>max-dn max-directory-numbers</code> 例: <code>Router(config-register-global)# max-dn 50</code>	このルータでサポートされるディレクトリ番号の数を制限します。 <ul style="list-style-type: none">最大数はプラットフォームとバージョンで異なります。値を表示するには ? と入力します。
手順 20	<code>max-pool max-voice-register-pools</code> 例: <code>Router(config-register-global)# max-pool 40</code>	Unified SRST ルータでサポートされる SIP 電話機の最大数を設定します。
手順 21	<code>exit</code> 例: <code>Router(config-register-global)# exit</code>	音声レジスタ グローバル コンフィギュレーション モードを終了します。
手順 22	<code>voice register pool pool-tag</code> 例: <code>Router(config)# voice register pool 1</code>	音声レジスタ プール コンフィギュレーション モードを開始して、SIP 電話機の電話機固有パラメータを設定します。
手順 23	<code>id { network address mask mask ip address mask mask mac address }</code> 例: <code>Router(config-register-pool)# id network 2001:420:54FF:13::901:0/117</code> <code>Router(config-register-pool)# id network 10.64.88.0 mask 255.255.255.0</code>	ある程度の認証をサポートするため、ローカルに使用可能な個々の SIP 電話機を明示的に識別します。
手順 24	<code>end</code> 例: <code>Router(config)# end</code>	特権 EXEC モードに戻ります。

SIP IP Phone の IPv6 プールの設定例

次の例は、SIP IP Phone の IPv6 プールの設定を示しています。

```
ipv6 unicast-routing
voice service voip
sip
no anat
call service stop
exit
exit
sip-ua
protocol mode dual-stack
exit
voice service voip
sip
no call service stop
exit
voice register global
default mode
max-dn 50
max-pool 40
exit
voice register pool 1
id network 2001:420:54FF:13::901:0/117
end
```

次の例は、Unified SRST でサポートされている IPv6 のインターフェイス設定を示しています。

```
configure terminal
interface GigabitEthernet0/0/1
ip address 10.64.86.229 255.255.255.0
negotiation auto
ipv6 address 2001:420:54FF:13::312:82/119
ipv6 enable
```

次の例は、Unified SRST でサポートされている IPv6 の IP ルート設定を示しています。

```
ipv6 route 2001:420:54FF:13::312:0/119 2001:420:54FF:13::312:1
ipv6 route 2001:420:54FF:13::901:0/119 2001:420:54FF:13::312:1
```

次の例は、SIP コール サービスを **call service stop CLI** コマンドでシャットダウンした際の出力を示しています。

```
Router# show sip service
SIP service is shut
under 'voice service voip', 'sip' submode
```

次の例は、SIP コール サービスを **no call service stop CLI** コマンドでアクティブにした際の出力を示しています。

```
Router# show sip-ua service
SIP Service is up
under 'voice service voip', 'sip' submode
```

Cisco Unified IP Phone およびプラットフォームのサポート

ここでは、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 CM 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 \(25 ページ\)](#)
- [Cisco Unified IP Phone のサポート \(25 ページ\)](#)
- [プラットフォームとメモリのサポート \(26 ページ\)](#)
- [Cisco Unified Communications Manager の互換性 \(26 ページ\)](#)
- [信号のサポート \(26 ページ\)](#)
- [言語のサポート \(26 ページ\)](#)
- [スイッチのサポート \(27 ページ\)](#)

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



(注)

Cisco IOS リリース 12.4(15)T では、各プラットフォームでサポートされる SIP 電話の数は、サポートされる SCCP 電話の数と等しくなっています。たとえば、3845 は、SIP か SCCP かにかかわらず、720 台の電話機をサポートするようになっています。

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

関連する互換性情報については、『[Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix](#)』を参照してください。

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、『[Compatibility Information](#)』を参照してください。

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。

Cisco Unified CM 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 Unified 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。

Unified SRST の IPv6 サポートでは、従来のすべての IP フォンと音声ゲートウェイは、SCCP シグナリングから IPv4 専用 SIP シグナリングに変換または再構成される必要があります(該当する場合)。

プラットフォームとメモリのサポート

プラットフォームとメモリのサポートに関する最新情報については、『[Compatibility Information](#)』を参照してください。

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 サポートに関連した更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 リリースをサポートしているプラットフォームは、そのプラットフォーム用のソフトウェア イメージがあるかどうかによります。一部のプラットフォームのソフトウェア イメージは、事前の通知なしに延期、遅延、または変更される場合があります。各 Cisco IOS ソフトウェア リリースのプラットフォーム サポートおよび利用可能なソフトウェア イメージの更新情報は、オンライン 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。

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、『[Compatibility Information](#)』を参照してください。

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 Unified Communications Manager Express Cisco Unified CME Localization Matrix](#)』を参照してください。

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)

次の作業

このマニュアルの次の各章では、Cisco Unified SIP SRST の設定方法について説明します。表 1-3 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が Cisco Unified SRST 用に正しく設定されていることを確認します。

表 1-3 Cisco Unified SRST の設定順序

作業	作業についての参照先
29. Cisco Unified SRST システムがネットワークと通信するための設定	ネットワークの設定(53 ページ)
30. バージョン 4.1 の機能の設定	Cisco Unified SIP SRST 4.1(65 ページ)
31. SCCP による Cisco Unified SRST Phone の基本的な設定	SCCP を用いた Cisco Unified IP Phone の設定(75 ページ)
32. 基本的なレジストラ サービスの提供による外部 SIP プロキシサーバへのバックアップの実現	SIP を用いた Cisco Unified IP Phone の設定(93 ページ)
33. 着信コールと発信コールの設定	コール処理の設定(109 ページ)
34. SRST のオプション セキュリティの設定	SCCP および SIP のセキュア SRST の設定(163 ページ)
35. ボイスメールの設定	ボイスメールと Cisco Unified SRST の統合(243 ページ)

表 1-3 Cisco Unified SRST の設定順序(続き)

作業	作業についての参照先
36. ビデオ パラメータの設定	ビデオ パラメータの設定(267 ページ)
37. Cisco Unified Survivable Remote Site Telephony (SRST) のモニタリングとメンテナンス	Cisco Unified SRST のモニタリングとメンテナンス(281 ページ)

その他の関連資料

ここでは、Cisco Unified SIP 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\(28 ページ\)](#)
- [標準\(29 ページ\)](#)
- [MIB\(30 ページ\)](#)
- [RFC\(30 ページ\)](#)
- [テクニカル サポート\(30 ページ\)](#)

関連資料

関連項目	ドキュメント
Cisco IOS 音声製品の設定	<ul style="list-style-type: none"> • 『Cisco IOS Voice Configuration Library』 • 『Cisco IOS Voice Command Reference』 • 『Cisco IOS Debug Command Reference』 • 『Cisco IOS Tcl IVR and VoiceXML Application Guide』 • 『Cisco IOS Survivable Remote Site Telephony Version 3.2 System Administrator Guide』
SRST および MGCP フォールバックの設定	<ul style="list-style-type: none"> • 『Configuring MGCP Gateway Support for Cisco Unified Communications Manager』 • 『MGCP Gateway Fallback Transition to Default H.323 Session Application』 • 『Configuring SRS Telephony and MGCP Fallback』
Cisco Unified Communications Manager のユーザ マニュアル	<ul style="list-style-type: none"> • 『Cisco Unified Communications Manager』 • 『Cisco Unified Communications Manager Security Guide』 • 『Cisco Unified Communications Operating System Administration Guide』

関連項目	ドキュメント
Cisco Unified IP Phone	<ul style="list-style-type: none"> 『Cisco 7900 Series Unified IP Phones End-User Guides』 『Cisco IP Phone Authentication and Encryption for Cisco Communications Manager』 『Cisco Unified IP Phone 7970 Series Administration Guide for Cisco Unified CallManager, Release 5.0 (for models 7970G and 7971G-GE) (SCCP)』、「Understanding Security Features for Cisco IP Phones」のセクション
Cisco Unified SRST コマンドおよび仕様	<ul style="list-style-type: none"> 『Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)』 『Cisco Unified SRST 8.0 Supported Firmware, Platforms, Memory, and Voice Products』 『Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products』
シスコのセキュリティのマニュアル	<ul style="list-style-type: none"> 『Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways』 『Cisco IOS Certificate Server』 『Manual Certificate Enrollment (TFTP and Cut-and-Paste)』 『Certification Authority Interoperability Commands』 『Certificate Enrollment Enhancements』
Cisco SIP SRST V3.4: Cisco IOS SIP Survivable Remote Site Telephony 機能のロードマップ	<ul style="list-style-type: none"> 『Cisco IOS SIP SRST Feature Roadmap』
Cisco SIP 機能	<ul style="list-style-type: none"> 『Cisco IOS SIP Configuration Guide』
Cisco SRST コマンド リファレンス	<ul style="list-style-type: none"> 『Cisco IOS Survivable Remote Site Telephony Version 3.2 Command Reference』
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 リファレンス情報	<ul style="list-style-type: none"> 『Cisco IOS Voice Command Reference』 『Cisco IOS Debug Command Reference』
DHCP	<ul style="list-style-type: none"> 『Cisco IOS DHCP Server』
メディア非アクティブ コール検出	<ul style="list-style-type: none"> 『Media Inactive Call Detection』
Cisco Unified SRST 用の電話機のマニュアル	<ul style="list-style-type: none"> 『Cisco Unified IP Phones 7900 Series』 『Survivable Remote Site Telephony』
標準的な用語集	<ul style="list-style-type: none"> 『Cisco IOS Voice Configuration Library Glossary』
標準的な前書き	<ul style="list-style-type: none"> 『Cisco IOS Voice Configuration Library Preface』

標準

標準	タイトル
ITU X. 509 バージョン 3	「Public-Key and Attribute Certificate Frameworks」

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2246	「The Transport Layer Security (TLS) Protocol Version 1.0」
RFC 2543	「SIP: Session Initiation Protocol」
RFC 3261	「SIP: Session Initiation Protocol」
RFC 3711	「The Secure Real-Time Transport Protocol (SRTP)」

テクニカル サポート

説明	リンク
シスコテクニカルサポートおよびドキュメンテーション Web サイトでは、製品、テクノロジー、ソリューション、テクニカルティップス、ツールへのリンクなど、技術的なコンテンツを検索可能な形で大量に提供しています。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/techsupport

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスや一般的なシスコのマニュアルについては、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。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>.



Cisco Unified Enhanced Survivable Remote Site Telephony

この章では、既存のクラシック Unified SRST と比べ、高度なサービスを提供する SRST 機能の拡張である、Unified Enhanced Survivable Remote Site Telephony (Unified E-SRST) 機能について説明します。

目次

- [Unified E-SRST の概要 \(31 ページ\)](#)
- [ボイス ハント グループのサポートがある Unified E-SRST \(32 ページ\)](#)
- [SIP: Unified E-SRST の設定 \(35 ページ\)](#)
- [SCCP: Unified E-SRST の設定 \(50 ページ\)](#)
- [Unified E-SRST のスケール サポート \(51 ページ\)](#)
- [次の作業 \(52 ページ\)](#)

Unified E-SRST の概要

Unified SRST Manager による Unified Communications Manager のための Unified E-SRST プロビジョニングは、Unified E-SRST リリース 12.2 以降ではサポートされません。Unified SRST Manager はリモートサイトのモニタ、レポート、トラブルシューティングに役立つ GUI ベースのツールです。これは、Unified Communications Manager と Unified E-SRST ゲートウェイの間で自動同期を実行するため、ダイヤルプラン マッピングを含む、ユーザと電話機の追加、削除、および変更役に役立ちます。また、すべてのリモートサイトを一元化して管理および制御します。

Unified E-SRST は、Unified Communications Manager に登録された電話機のフォールバックをサポートするために、CLI コマンドを使用してプロビジョニングされます。

Unified-ESRST の利点

Unified E-SRST を設定すると、従来の Unified SRST と比較して次のような機能上の利点があります。

- 音声ハント グループ
 - 共用回線
 - 混合共有回線(SIP 電話と SCCP 電話)
 - ハント統計情報の収集
 - 混合導入(SIP 電話と SCCP 電話)
- 共有回線
- BLF
- ビデオ
- B-ACD

Unified E-SRST での VHG の設定の詳細については、[ボイス ハント グループのサポートがある Unified E-SRST \(32 ページ\)](#)を参照してください。Unified E-SRST での共有回線、BLF、およびビデオの設定の詳細については、[SIP: Unified E-SRST の設定 \(35 ページ\)](#)を参照してください。

ボイス ハント グループのサポートがある Unified E-SRST

Unified E-SRST リリース 12.2 から、Cisco Unified Enhanced Survivable Remote Site Telephony (Unified E-SRST) を使用するボイス ハント グループのサポートが導入されました。この導入は、SIP 電話と SCCP 電話でサポートされます。Cisco IP Phone 7800 および 8800 シリーズは、この導入でサポートされる SIP 電話です。ボイス ハント グループ強化のための Unified E-SRST 導入は、Cisco 4000 シリーズ サービス統合型ルータで実施されます。

強化の一環として、ボイス ハント グループ機能は E-SRST モードでサポートされます。シーケンシャル、並列、最長アイドル、およびピア コールブラストのボイス ハント グループ導入は、Unified E-SRST 12.2 以降でサポートされます。

WAN の停止時に、Cisco Unified Communications Manager (Unified Communications Manager) 上の SIP Phone は、**mode esrst** の Unified E-SRST ルータにフォールバックします。このシナリオでは、SIP Phone はデフォルトではハント グループにログインします。ただし、CLI コマンド **members logout** がボイス ハント グループ設定モードで設定される場合、電話機はログアウト状態になります。Unified E-SRST モードで、Unified E-SRST にフォールバックする電話機は、機能アクセスコード (FAC) を介して HLog を使用して、状態を切り替えてボイス ハント グループにログイン (またはログアウト) できます。DN ステータス (ログインまたはログアウト) は、Unified E-SRST に登録されている電話機に表示されます。次の FAC コードは、Unified E-SRST に導入される拡張の一部として使用できます。

- FAC 標準 (コード: *5)
- FAC カスタム (コード: カスタマイズ可能。最大文字列長は 10 です。たとえば、*89,
- 8888888888 など)

複数回線がある電話機からユーザが FAC を入力するときに、共通音声レジスタ プール設定がある導入と個別音声レジスタ プール設定がある導入とでログアウト動作が異なることが知られています。

- 共通音声レジスタ プール設定:DN は電話機のレベルではなく、個別にログアウトします。
- 個別音声レジスタ プール設定:ユーザによる FAC 入力の提供元の DN(プライマリ、セカンダリなど)に関係なく、DN は電話機レベルでログアウトします。

WAN が使用可能な場合、電話機は Unified Communications Manager に登録し直されます。ボイスハントグループが強化された Unified E-SRST の設定例については、[ボイスハントグループが強化された Unified E-SRST の設定例\(45 ページ\)](#)を参照してください。

Unified E-SRST リリース 12.2 では、共有回線と混合共有回線(SCCP 電話と SIP 電話)があるボイスハントグループのサポートが導入されています。ボイスハントグループでサポートされている混合共有回線の場合、個々の音声レジスタ プールのみを設定できます。共通音声レジスタ プールはサポートされていません。Unified E-SRST 上の音声ハントグループに対して設定される混合共有回線の設定例については、[Unified E-SRST でのボイスハントグループとの共有回線の設定例\(47 ページ\)](#)を参照してください。

また、ハント統計収集も Unified E-SRST 12.2 以降のリリースでサポートされます。

SIP 電話と SCCP 電話の混合導入は Unified E-SRST リリース 12.2 でサポートされます。SIP 電話と SCCP 電話の混合導入からのハントグループログアウトは、以下を使用してサポートされます。

- FAC
- 機能ボタン、または
- DND

回線レベルのログアウトと電話機レベルのログアウトは、FAC(*4)を使用してサポートされます。



(注)

共有回線では、ハントグループのログアウトはサポートされません。共有回線はログイン状態を保持します。

Unified E-SRST での B-ACD のサポート

B-ACD は、リリース 12.2 で導入された Unified E-SRST 導入の一環としてサポートされます。**mode esrst** の Unified E-SRST ルータにフォールバックする SIP 電話の場合、CLI コマンド **members logout** が設定されていることを確認する必要があります。メンバーログアウト機能は、FAC を使用して電話機からログインし直します。また、B-ACD からボイスハントグループへのコール配信もサポートします。

設定例については、[Unified E-SRST での B-ACD の設定例\(46 ページ\)](#)を参照してください。

Unified E-SRST でのボイス ハント グループ設定の推奨事項

ボイス ハント グループのサポートがある Unified E-SRST リリースには、次の設計特性があります。

- Unified Communications Manager からフォールバックするすべてのディレクトリ番号に対して、この導入では共通音声レジスタ プール設定と個別音声レジスタ プール設定がサポートされます。個別の **voice register pool** は、CLI コマンド **id device-id-name** で、**voice register dn** 設定を指定して設定することをお勧めします。
- 電話機が Unified E-SRST にフォールバックするように、CLI コマンド **mode esrst** は必ず **voice register global** 設定モードの下で設定します。
- 個別音声レジスタ プール設定がある導入に対しては必ず、CLI コマンド **id ip** または **id device-id-name** を、**voice register dn** 設定を指定して、**voice register pool** 設定モードの下で設定します。設定例については、[ボイス ハント グループが強化された Unified E-SRST の設定例\(45 ページ\)](#)を参照してください。
- 電話機の IP アドレスが、電話機に設定された DHCP により変更される可能性があるシナリオでは、CLI コマンド **id device-id-name** は、**voice register pool** 設定モードの下で設定される CLI コマンドとしての **id ip** に優先することを確認します。
- 共通音声レジスタ プール設定がある導入の **voice register pool** 設定モードの下で、CLI コマンド **id network** が設定されていることを確認します。Unified Communications Manager から Unified E-SRST にフォールバックする電話機の登録を促進する推奨設定は、**id network 8.55.0.0 255.255.0.0** です。
- CLI コマンド **members logout** が、**voice hunt-group** 設定モードの下で設定されていることを確認します。SIP 電話が Unified Communications Manager から Unified E-SRST にフォールバックするときには、CLI がデフォルトで適用されます。
- CLI コマンド **fac standard** が、**telephony-service** 設定モードの下で設定されていることを確認します。*5 以外の FAC コードを設定する場合は、CLI コマンド **fac custom** を **telephony-service** 設定モードの下で設定する必要があります。
- CLI コマンド **call-park system application** および **hunt-group logout hlog** が、**telephony-service** 設定モードの下で設定されていることを確認します。CLI コマンドは、FAC 機能が動作するための必須の設定です。

音声ハント グループを Unified E-SRST 上で設定する手順については、[Unified E-SRST でのボイス ハント グループの設定\(40 ページ\)](#)を参照してください。

Unified E-SRST 上の音声ハント グループの設定例については、[ボイス ハント グループが強化された Unified E-SRST の設定例\(45 ページ\)](#)を参照してください。

Unified E-SRST リリース 12.2 の制限事項

ボイス ハント グループがある Unified E-SRST 導入には、次の制約事項があることが知られています。

- 自動ログアウトはサポートされません。
- プログラム可能なライン キー (PLK) はサポートされません
- HLog ソフトキーはサポートされません。

SIP: Unified E-SRST の設定

Cisco Unified SIP IP 電話対応の Enhanced SRST 機能は、SIP 電話と ESRST との間でのバージョン ネゴシエーションをサポートし、Cisco Unified ESRST モードでより多くの機能を有効にします。現在のシナリオでは、SIP 電話が SRST モードにフォールバックすると、共有回線、話中ランプ フィールド (BLF)、ビデオ コールなどの機能は、機能が SRST モードでサポートされていないため、電話では無効になります。ただし、Enhanced Survivable Remote Site Telephony (E-SRST) 展開では、バージョン ネゴシエーションを使用して次の機能を有効にすることができます。

- 共有回線
- ビジー ランプ フィールド (BLF)
- ビデオ コール

表 2-1 に、E-SRST モードでサポートされる機能と機能の予期される動作の一覧を示します。

表 2-1 E-SRST モードでサポートされる機能

機能	サポートされる機能	E-SRST モードの予期される動作
共有回線	C 割り込み	未サポート (フェールオーバーの後、電話はキーを保持しません。)
	Privacy-on-hold	サポート対象
	転送	サポート対象
	会議	サポート対象
BLF	BLF dn モニタリング	サポート対象
	BLF デバイススペースのモニタリング	未サポート (RT 電話で未サポート)
	BLF コールリストのモニタリング	サポート対象
	コールパーク スロットのモニタリング	未サポート
	ページング dn のモニタリング	未サポート
	会議 dn のモニタリング	未サポート

- ESRST と 電話との間のバージョン ネゴシエーション機能を有効にするには、音声レジスタ グローバル モードで「mode esrst」を設定する必要があります。
- SRST Manager を使用して、ESRST ブランチ ルータの CLI プロビジョニングを自動化することをお勧めします。

SRST の詳細については、『Cisco Unified SRST Manager Administration Guide』を参照してください。

制約事項

- バージョン ネゴシエーション機能は、Cisco Unified 9951、9971、8961 SIP IP Phone、Cisco IP Phone 7800 および 8800 シリーズでのみサポートされます。
- 電話のファームウェア バージョンは、バージョン 9.4.1 以降です。
- この機能は、SRST のフェールオーバー中に、ローカル Cisco Unified SIP IP 電話と非時分割多重 (TDM) ビデオ通話との間でのみビデオ コールをサポートします。
- 共有回線と BLF 動作などの電話固有の機能を有効にするには、個々の音声レジスタ プールを設定する必要があります。

E-SRST モードの有効化

E-SRST モードのバージョン ネゴシエーション機能を有効にするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **mode esrst**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
手順 1	enable 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。
手順 2	configure terminal 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	voice register global 例: Router(config)# voice register global	音声レジスタ グローバル コンフィギュレーション モードを開始して、Cisco Unified CME でサポートされるすべての SIP 電話に対してパラメータを設定します。
手順 4	mode esrst 例: Router(config-register-global)# mode esrst	音声レジスタ グローバル モードで E-SRST モードを設定します。
手順 5	exit 例: Router(config-register-global)# exit	音声レジスタ グローバル コンフィギュレーション モードを終了します。

SIP 共有回線の設定

SIP 共有回線を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **number** *number*
5. **shared-line** [**max-calls** *number-of-calls*]
6. **huntstop channel** *number-of-channels*
7. **end**

BLF の設定

BLF を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **presence enable**
5. **exit**
6. **presence**
7. **max-subscription** *number*
8. **presence call-list**
9. **end**

電話番号の表示の有効化

電話番号が表示されるようにするには、次の手順を実行します。

1. **voice register dn** *dn-tag*
2. **number** *number*
3. **allow watch**
4. **end**

音声レジスタ プールのBLFの有効化:

音声レジスタ プールの BLF を有効にするには、次の手順を実行します。

1. **enable**
2. **configure terminal**
3. **voice register pool *pool-tag***
4. **number *tag dn dn-tag***
5. **blf-speed-dial *tag number label string [device]***
6. **presence call-list** (不在着信/受信済み/発信済みのすべてのコールに対してプレゼンス機能を有効にするため)
7. **end**

詳細については、『[Cisco Unified Communications Manager Administration Guide](#)』を参照してください。

例: ESRST モード

次の例は、E-SRST モードを有効にする方法を示しています。

```
Router# configure terminal
Router(config)# voice register global
Router(config-register-global)# mode esrst
```

例: 共有回線の設定

次の例は、共有回線を構成する方法を示しています。

```
Router(config)#voice register dn 1
Router (config-register-dn)#number 1111
Router (config-register-dn)#shared-line

Router(config)#voice register pool 1
Router(config-register-pool)#Id mac 002D.264E.54FA
Router(config-register-pool)#type 9971
Router(config-register-pool)#number 1 dn 1

Router(config)#voice register pool 2
Router(config-register-pool)#id mac 000D.39F9.3A58
Router(config-register-pool)#type 7965
Router(config-register-pool)#number 1 dn 1
```

例: BLF の設定

次の例は、BLF を設定する方法を示しています。

```
Router(config)#voice register dn 1
Router (config-register-dn)#number 1111
Router (config-register-dn)#allow watch

Router(config)#voice register dn 1
Router (config-register-dn)#number 2222

Router(config)#voice register pool 1
Router(config-register-pool)#id mac 0015.6247.EF90
Router(config-register-pool)#type 7971
```

```
Router(config-register-pool)#number 1 dn 1

Router(config)#voice register pool 2
Router(config-register-pool)#id mac 0012.0007.8D82
Router(config-register-pool)#type 7912
Router(config-register-pool)#number 1 dn 2
Router(config-register-pool)#blf-speed-dial 1 1111 label "1111"
```



(注) 電話と ESRST ルータが異なるサブネットに属している場合、ユーザは、ESRST の音声レジスタプールで CUCM、ユーザ名、パスワードの構成にダイジェスト クレデンシャルを設定する必要があります。

CUCM のダイジェスト クレデンシャルの設定

CUCM でユーザ名とパスワードにダイジェスト認証を設定するには、次の手順を実行します。

-
- 手順 1 Cisco Unified Communications Manager にログインします。
- 手順 2 [システム(System)] > [セキュリティ(Security)] > [電話セキュリティ プロファイル(Phone Security Profile)] の順に移動します。
- 既存の構成を編集するか、または新しい構成を作成して電話に関連付けます。
 - [ダイジェスト認証を有効にする(Enable Digest Authentication)] チェックボックスをオンにします。
- 手順 3 [ユーザ管理(User Management)] > [エンド ユーザ(End User)] に移動します。
- 新規ユーザを作成します。
 - ユーザ ID およびダイジェスト クレデンシャルを追加します。
- 手順 4 [電話の設定(Phone Settings)] ページに移動し、[ダイジェスト ユーザ(Digest User)] フィールドでユーザを関連付けます。
-

ESRST でのダイジェスト クレデンシャルの設定

特定の音声レジスタ プールでクレデンシャルを設定するには、次の手順を実行します。

手順の概要

- enable
- configure terminal
- voice register pool <pool-tag>
- username <username> password <password>
- end

例: ESRST でのダイジェスト クレデンシャルの設定

次の例は、ESRST にダイジェスト クレデンシャルを設定する方法を示しています。

```
Router# conf terminal
Router(config)#voice register pool 10
Router (config-register-pool)# username abc password xyz
```

Unified E-SRST でのボイス ハント グループの設定

Unified E-SRST モードの音声ハント グループ機能を有効にするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **mode esrst**
5. **max-ephones** *max-phones*
6. **max-dn** *max-directory-numbers*
7. **ip source-address** *ip-address* [**port** *port*] [**any-match** | **strict-match**]
8. **call-park system application**
9. **hunt-group logout HLog**
10. **transfer-system full-consult**
11. **transfer-pattern** *transfer-pattern*
12. **fac standard**
13. **create cnf-files**
14. **exit**
15. **voice register global**
16. **mode esrst**
17. **max-dn** *max-directory-numbers*
18. **max-pool** *max-phones*
19. **exit**
20. **voice register pool 1**
21. **id** [**network** *address mask mask* | **ip** *address mask mask*][**device-id-name** *devicename*]
22. **dtmf-relay rtp-nte**
23. **exit**
24. **voice hunt-group hunt-tag** {**longest-idle** | **parallel** | **peer** | **sequential**}
25. **members logout**
26. **list** *number* [, *number...*]
27. **timeout** *seconds*
28. **statistics collect**
29. **pilot 1111**

手順の詳細

	コマンドまたはアクション	目的
手順 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。
手順 2	<code>configure terminal</code> 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	<code>telephony-service</code> 例: Router(config)# telephony-service	telephony-service コンフィギュレーション モードを開始します。
手順 4	<code>mode esrst</code> 例: Router(config)# telephony-service	telephony-service 設定モードで E-SRST モードを設定します。
手順 5	<code>max-ephones max-phones</code> 例: Router(config-telephony)# max-ephones 40	ルータがサポートできる 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。
手順 6	<code>max-dn max-directory-numbers</code> 例: Router(config-telephony)# max-dn 15	ルータがサポートできる電話番号(DN)の最大数を設定します。 • <i>max-directory-numbers</i> : ルータがサポートできる最大数の電話番号(DN)または仮想音声ポート。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。
手順 7	<code>ip source-address ip-address [port port] [any-match strict-match]</code> 例: Router(config-telephony)# ip source-address 8.39.23.24 port 2000	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 アドレスの検証をサポートします。デフォルトのポート番号は 2000 です。
手順 8	<code>call-park system {application redirect}</code> 例: Router(config-telephony)# call-park system application	コールパーク機能のシステムパラメータを定義します。 • <i>application</i> : Unified SRST でサポートされるコールパーク機能を有効にします。
手順 9	<code>hunt-group logout {DND HLog}</code> 例: Router(config-telephony)# hunt-group logout HLog	telephony-service 設定モードで、hunt-group logout のオプションと Hlog を設定します。

■ ボイス ハント グループのサポートがある Unified E-SRST

	コマンドまたはアクション	目的
手順 10	<code>transfer-system full-consult</code> 例: Router(config-telephony)# transfer-system full-consult	コール転送方法を指定します。 • full-consult : 使用可能な場合、H.450.2 標準の方法と 2 番目の電話回線を使用するコンサルトが行われてコールが転送されます。2 番目の回線を使用できない場合、コールは full-blind にフォールバックします。
手順 11	<code>transfer-pattern transfer-pattern</code> 例: Router(config-telephony)# transfer-pattern .T	Cisco Unified IP Phone で、指定された電話番号パターンにコールを転送できるようにします。転送パターンが設定されていない場合、デフォルトでは他のローカル IP Phone だけで転送が許可されます。 • transfer-pattern : 許可されるコール転送の数字列。
手順 12	<code>fac { standard custom { alias alias-tag feature } }</code> 例: Router(config-telephony)# fac standard	すべての標準機能アクセス コード (FAC) を有効にするか、または telephony-service 設定モードで個々のカスタム FAC を作成して有効にします。
手順 13	<code>create cnf-files</code> 例: Router(config-telephony)# create cnf-files version-stamp	telephony-service 設定モードで、IP フォンに必要な XML (eXtensible Markup Language) 設定ファイルを構築します。
手順 14	<code>exit</code> 例: Router(config-telephony)# exit	Telephony-service コンフィギュレーション モードを終了します。
手順 15	<code>voice register global</code> 例: Router(config)# voice register global	音声レジスタ グローバル コンフィギュレーション モードを開始します。
手順 16	<code>mode esrst</code> 例: Router(config-register-global)# mode esrst	音声レジスタ グローバル モードで E-SRST モードを設定します。
手順 17	<code>max-dn max-directory-numbers</code> 例: Router(config-register-global)# max-dn 40	音声レジスタ グローバル コンフィギュレーション モードの Cisco ルータでサポートされている、SIP 電話のディレクトリ番号 (内線番号) の最大数を設定します。
手順 18	<code>max-pool max-phones</code> 例: Router(config-register-global)# max-pool 40	Unified SRST ルータでサポートされる SIP 電話機の最大数を設定します。 • バージョンとプラットフォームに依存します。範囲を表示するには、? と入力します。
手順 19	<code>exit</code> 例: Router(config-register-global)# exit	音声レジスタ グローバル コンフィギュレーション モードを終了します。

コマンドまたはアクション	目的
<p>手順 20 <code>voice register pool pool-tag</code></p> <p>例: Router(config)# voice register pool 1</p>	<p>音声レジスタ プール コンフィギュレーション モードを開始して、SIP 電話機の電話機固有パラメータを設定します。</p>
<p>手順 21 <code>id [{network address mask mask ip address mask mask mac address}] [device-id-name devicename]</code></p> <p>例: Router(config-register-pool)# id network 8.55.0.0 mask 255.255.0.0</p>	<p>ローカルに使用できる個別の SIP IP Phone またはそのセットを明示的に識別します。キーワードと引数が次のように定義されます。</p> <ul style="list-style-type: none"> • network address mask mask: network address mask mask のキーワードと引数の組み合わせは、指示された IP サブネット内の任意の IP Phone から指示された電話番号に対して SIP 登録メッセージを受け入れるために使用されます。 • ip address mask mask: ip address mask mask のキーワードと引数の組み合わせは、個別の電話機を識別するために使用されます。 • mac address: 特定の Cisco Unified IP Phone の MAC アドレスです。 • device-id-name devicename: 電話の設定ファイルのダウンロードに使用するデバイス名を定義します。
<p>手順 22 <code>dtmf-relay rtp-nte</code></p> <p>例: Router(config-register-pool)# dtmf-relay rtp-nte</p>	<p>Real-Time Transport Protocol (RTP) と Named Telephony Event (NTE) ペイロード タイプを使用して DTMF トーンを転送し、RFC 2833 標準方式を使用して DTMF リレーをイネーブルにします。</p>
<p>手順 23 <code>exit</code></p> <p>例: Router(config-register-pool)# exit</p>	<p>音声レジスタ プール コンフィギュレーション モードを終了します。</p>

コマンドまたはアクション	目的
<p>手順 24 <code>voice hunt-group hunt-tag {longest-idle parallel peer sequential}</code></p> <p>例: Router(config)# voice hunt-group 1 sequential</p>	<p>音声ハント グループ コンフィギュレーション モードを開始して、ハント グループを定義します。</p> <ul style="list-style-type: none"> • <code>hunt-tag</code>: 設定するハント グループの一意のシーケンス番号。範囲は 1 ~ 100 です。 • <code>longest idle</code>: 最も長い時間アイドル状態であったディレクトリ番号にコールを送るようにするハント グループ。 • <code>sequential</code>: ディレクトリ番号がリストされている順序で左から右に呼び出されるようにするハント グループ。 • <code>並列</code>: すべてのディレクトリ番号が同時に呼出音を鳴らすハント グループ。 • <code>ピア</code>: あるディレクトリ番号に発信されたコールが、回線の次のディレクトリ番号に対して呼出音を鳴らすハント グループ。 <p>ハント グループのタイプを変更するには、最初にこのコマンドの <code>no</code> 形式を使用して既存のハント グループを削除してから、グループを再作成します。</p>
<p>手順 25 <code>members logout</code></p> <p>例: Router(config-voice-hunt-group)# members logout</p>	<p>Hlogout 初期状態のボイス ハント グループ内のすべての非共有静的メンバーまたはエージェントに対して、Unified SRST システムを設定します。</p>
<p>手順 26 <code>list number [, number...]</code></p> <p>例: Router(config-voice-hunt-group)# list 1812, 1813, 1814</p>	<p>音声ハント グループのメンバーとなる内線番号のリストを定義します。</p>
<p>手順 27 <code>timeout seconds</code></p> <p>例: Router(config-voice-hunt-group)# timeout 30</p>	<p>コールに応答がない場合に、何秒後に音声ハント グループ リスト内の次の番号にリダイレクトされるかを定義します。</p>
<p>手順 28 <code>statistics collect</code></p> <p>例: Router(config-voice-hunt-group)# statistics collect</p>	<p>音声ハント グループのコール統計情報の収集をイネーブルにします。</p>
<p>手順 29 <code>exit</code></p> <p>例: Router(config-voice-hunt-group)# exit</p>	<p>音声ハント グループ コンフィギュレーション モードを終了します。</p>

ボイス ハント グループが強化された Unified E-SRST の設定例

以下に示すのは、共通音声レジスタ プール設定がある導入に対する、**telephony-service**、**voice register global**、**voice register pool**、および **voice hunt-group** 設定モードの下での Unified E-SRST リリース 12.2 の設定例です。

```
Router#
telephony-service
call-park system application
hunt-group logout HLog
transfer-system full-consult
fac standard

Router#sh run | sec global
voice register global
mode esrst
max-dn 40
max-pool 40

Router#
voice register pool 1
id network 8.55.0.0 mask 255.255.0.0
dtmf-relay rtp-nte
Router#
telephony-service
max-ephones 40
max-dn 50
ip source-address 8.39.23.24 port 2000
call-park system application
transfer-system full-consult
transfer-pattern .T
fac standard
create cnf-files version-stamp Jan 01 2002 00:00:00

Router#sh run | sec hunt
voice hunt-group 1 sequential
members logout
list 1812,1813,1814
timeout 30
statistics collect
pilot 1111
```

以下に示すのは、個別音声レジスタ プール設定がある導入に対する、設定された CLI コマンド **id ip** を使用した、Unified E-SRST リリース 12.2 の設定例です。

```
voice register dn 2
  number 4000
!
voice register dn 3
  number 4002
!
voice register pool 2
busy-trigger-per-button 2
  id ip 8.55.0.241 mask 255.255.0.0
  type 8811
  number 1 dn 2
  dtmf-relay rtp-nte
  codec g711ulaw
!
voice register pool 3
  busy-trigger-per-button 2
  id ip 8.55.0.242 mask 255.255.0.0
```

```

type 7861
number 1 dn 3
dtmf-relay rtp-nte
codec g711ulaw

```

以下に示すのは、個別音声レジスタプール設定がある導入に対する、設定された CLI コマンド **id device-id-name** を使用した、Unified E-SRST リリース 12.2 の設定例です。

```

voice register dn 2
  number 4000
!
voice register dn 3
  number 4002
!
voice register pool 2
  busy-trigger-per-button 2
  id device-id-name SEP00EBD5CD77ED
  type 8811
  number 1 dn 2
  dtmf-relay rtp-nte
  codec g711u;aw

voice register pool 3
  busy-trigger-per-button 2
  id device-id-name SEP0076861A7EDC
  type 7861
  number 1 dn 3
  dtmf-relay rtp-nte
  codec g711ulaw

```

Unified E-SRST での B-ACD の設定例

以下に示すのは、Unified E-SRST でサポートされる B-ACD 機能の設定例です。

```

application
service aa-bcd bootflash:/app-b-acd-aa-3.0.0.4_thd_v4.tcl
param space english index 0
param second-greeting-time 60
param welcome-prompt _bacd_welcome.au
param call-retry-timer 8
param voice-mail 1811
param space english language en
param max-time-call-retry 16
param service-name callq
param number-of-hunt-grps 2
param handoff-string aa-bcd
param space english location flash:
param max-time-vm-retry 2
param aa-pilot 1117
!
service clid_col_npw_npw
param uid-length 4
!
service aa-ccd bootflash:/app-b-acd-aa-3.0.0.4_thd_v4.tcl
param space english index 0
param drop-through-prompt _bacd_welcome.au
param second-greeting-time 60
param space english language en
param call-retry-timer 8
param voice-mail 1811
param max-time-call-retry 16

```

```
param service-name callq
param number-of-hunt-grps 1
param drop-through-option 1
param space english location flash:
param handoff-string aa-ccd
param max-time-vm-retry 2
param aa-pilot 1118
!
service callq bootflash:/imanager-b-acd-3.0.0.4_Q60.tcl
param queue-len 1
param aa-hunt1 1111
param number-of-hunt-grps 4
param queue-manager-debug 1
!
call-park system application
```

Unified E-SRST でのボイス ハント グループとの共有回線の設定例

次に示すのは、ボイス ハント グループ導入で混合共有回線(SIP 電話と SCCP 電話)のサポートがある Unified E-SRST リリース 12.2 の設定例です。

```
Router# sh run | sec global
voice register global
  mode esrst
  no allow-hash-in-dn
  max-dn 40
  max-pool 40

Router# sh run | sec pool
max-pool 40
voice register pool 1
  busy-trigger-per-button 2
  id device-id-name SEP00CCFC4AA4DC
  type 8811
  number 1 dn 1
  number 2 dn 21
  dtmf-relay rtp-nte
  username xxxx password uvwx
  codec g711ulaw
  no vad
voice register pool 2
  busy-trigger-per-button 2
  id device-id-name SEP00CCFC177A4E
  type 8841
  number 1 dn 2
  dtmf-relay rtp-nte
  username xxxx password uvwx
  codec g711ulaw
  no vad
voice register pool 3
  busy-trigger-per-button 2
  id device-id-name SEP0076861ADEF0
  type 7841
  number 1 dn 3
  number 2 dn 22
  dtmf-relay rtp-nte
  username xxxx password uvwx
  codec g711ulaw
  no vad
voice register pool 4
  busy-trigger-per-button 2
  id device-id-name SEP00EBD5CD270C
```

```
type 8811
number 1 dn 4
number 2 dn 22
dtmf-relay rtp-nte
username xxxx password uvwx
codec g711ulaw
no vad
voice register pool 5
  busy-trigger-per-button 2
  id device-id-name SEP94D4692A2553
  type 8841
  number 1 dn 5
  dtmf-relay rtp-nte
  username xxxx password uvwx
  codec g711ulaw
  no vad
voice register pool 6
  busy-trigger-per-button 2
  id device-id-name SEP00CAE540C4B5
  type 8811
  number 1 dn 6
  number 2 dn 21
  dtmf-relay rtp-nte
  username xxxx password uvwx
  codec g711ulaw
  no vad
alias exec pool show voice register pool all br
```

```
Router# sh run | sec dn
no allow-hash-in-dn
max-dn 40
voice register dn 1
  voice-hunt-groups login
  number 1811
voice register dn 2
  voice-hunt-groups login
  number 1812
voice register dn 3
  voice-hunt-groups login
  number 1813
voice register dn 4
  voice-hunt-groups login
  number 1814
voice register dn 5
  voice-hunt-groups login
  number 1815
voice register dn 6
  voice-hunt-groups login
  number 1816
voice register dn 21
  voice-hunt-groups login
  number 1821
  shared-line
voice register dn 22
  voice-hunt-groups login
  number 1822
  shared-line
```

```
Router# sh run | sec ephone
max-ephones 40
ephone-dn 11
  number 1911
ephone-dn 12
```

```
number 1912
ephone-dn 13
  number 1913
ephone-dn 14
  number 1914
ephone-dn 21
  number 1921
ephone-dn 22
  number 1822
  shared-line sip
ephone 11
  device-security-mode none
  mac-address 1111.1111.1911
  feature-button 1 HLog
  type 7970
  button 1:11
ephone 12
  device-security-mode none
  mac-address 1111.1111.1912
  feature-button 1 HLog
  type 7970
  button 1:12 2:21
ephone 13
  device-security-mode none
  mac-address 1111.1111.1913
  feature-button 1 HLog
  type 7970
  button 1:13 2:21
ephone 14
  device-security-mode none
  mac-address 1111.1111.1914
  feature-button 1 HLog
  type 7970
  button 1:14 2:22
alias ephone show ephone summary brief
alias exec ephone show ephone summary brief
```

```
Router# sh run | sec tele
telephony-service
  conference transfer-pattern
  mode esrst
  max-ephones 40
  max-dn 50
  ip source-address 8.39.23.24 port 2000
  service phone sshAccess 0
  service phone webAccess 0
  max-conferences 8 gain -6
  call-park system application
  hunt-group logout HLog
  transfer-system full-consult
  fac standard
```

SCCP: Unified E-SRST の設定

SCCP 電話の ESRST モードを有効にするには、telephony-service モードで mode esrst を設定する必要があります。

前提条件

- Cisco Unified CME 10.5 以降のバージョン
- telephony-services コマンドが設定されている必要があります。



(注)

SCCP 電話の場合、CME-as-SRST モードは **srst mode auto-provision** コマンドを使用してプロビジョニングされます。10.5 リリース以降、このコマンドは非推奨となります。CME-as-SRST モードの設定を試みると、次のメッセージが表示されます。
“Note: This configuration is being deprecated. Please configure “mode esrst” to use the enhanced SRST mode” (注: この構成は非推奨です。Enhanced SRST モードを使用するには、「mode esrst」を設定してください。)

手順の概要

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **mode esrst**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
手順 1	enable 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。
手順 2	configure terminal 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	telephony-service 例: Router(config)# telephony-service	telephony-service コンフィギュレーション モードを開始します。
手順 4	mode esrst 例: Router(config-telephony)# mode esrst	Telephony-service モードで E-SRST モードを設定します。
手順 5	exit 例: Router(config-telephony)# exit	Telephony-service コンフィギュレーション モードを終了します。

例:Enhanced SRST モードの構成

次の例は、E-SRST モードのデバイスのステータスを表示しています。

```
show telephony-service

CONFIG (Version=10.5)
=====
Version 10.5
Max phoneload sccp version 17
Max dspfarm sccp version 18
Cisco Unified Enhanced SRST
```



(注) SCCP 電話の場合、CME と ESRST の間でモードを切り替えると、CME または ESRST の構成全体がワイプされます (ephone、DN、テンプレートなどを含む)。

Unified E-SRST のスケール サポート

Unified E-SRST 10.5 から 12.0 では、Unified E-SRST モードのスケールは、SIP 電話と SCCP 電話の両方のクラシック SRST のスケールに対応するように増やされています。

表 2-2 は、リリース 10.5 から 12.0 の ESRST モードでサポートされる電話機数と DN のスケールをリストしています。

表 2-2 すべてのプラットフォームでサポートされる ESRST のスケール

プラットフォーム	新しい電話のスケール	新しい DN のスケール
Cisco 2901	35	200
Cisco 2911	50	300
Cisco 2921	100	400
Cisco 2951	250	500
Cisco 3925	730	1000
Cisco 3945	1200	1800
Cisco 3925E	1350	2000
Cisco 3945E	1500	2500
Cisco 4451-X	1500	2500
ISR 4321	35	200
ISR 4331	100	400
ISR 4351	730	1000
ISR 4431	1200	1800
ISR 4451	1500	2500



(注) 表に記載されているスケールの増加は、基本的なコールのみのものです。共有回線、BLF、ビデオ、および VHG など拡張機能サポートには、これらの数字は適用されません。

例: ESRST スケールの増加

次の例は、ISR 3945E プラットフォームの E-SRST モードでのスケール サポートの増加を示しています。

```
ESRST_3945e(config-telephony)#max-dn ?
<1-2500> Maximum single/dual/octo line directory numbers supported
ESRST_3945e(config-telephony)#max-ephones ?
<1-1500> Maximum phones to support
```

次の作業

[「ネットワークの設定」セクション\(53 ページ\)](#)に進んでください。



ネットワークの設定

この章では、Cisco Unified Communications Manager のフォールバックの間に DHCP を実行し、IP Phone と通信するために Cisco Unified Survivable Remote Site Telephony (SRST) ルータを設定する方法を説明します。

目次

- [ネットワークの設定に関する情報\(53 ページ\)](#)
- [ネットワークの設定方法\(54 ページ\)](#)
- [次の作業\(64 ページ\)](#)

ネットワークの設定に関する情報

WAN リンクに障害が発生すると、Cisco Unified IP Phone は Cisco Unified CM からキープアライブ パケットを受信していないことを検出します。次に Cisco Unified IP Phone をルータに登録します。Cisco Unified SRST ソフトウェアは自動的にアクティブになり、接続されたすべての Cisco Unified IP Phone のローカルデータベースを作成します(設定された最大数まで)。IP Phone は、中央 Cisco Unified CM がキープアライブ パケットの確認応答を行わなかった場合に、バックアップ コール処理ソースとしてルータを照会するように設定されています。Cisco Unified SRST ルータがコールの設定と処理、コールのメンテナンスとコールの終了を実施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 ブランチ オフィスでは、DHCP サービスは SRST ルータ自体によって、または DHCP リレーを使用して Cisco Unified SRST ルータを介して提供されます。DHCP の設定は、ネットワーク通信の設定における 2 つの主なタスクのうちの 1 つです。もう 1 つのタスクは、Cisco IP Phone から指定した IP アドレスによってメッセージを受信するように Cisco Unified SRST ルータを設定することです。キープアライブの間隔もこのときに設定します。

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 ルーティングのイネーブル化 \(54 ページ\)](#) (必須)
- [MGCP ゲートウェイでの Cisco Unified SRST のイネーブル化](#) (必須)
- [Cisco Unified SRST Phone での DHCP の設定 \(60 ページ\)](#) (必須)
- [キープアライブ インターバルの指定 \(63 ページ\)](#) (任意)

IP ルーティングのイネーブル化

SRST サービスを開始するには、IP ルーティング コマンドをイネーブルにして、使用またはバインドしたいインターフェイスを設定する必要があります。IP ルーティングをイネーブルにする方法については、「[Configuring IP Addressing](#)」を参照してください。

MGCP ゲートウェイでの Cisco Unified SRST のイネーブル化

SRST をフォールバック モードとして MGCP ゲートウェイと一緒に使用するには、SRST および MGCP フォールバックの両方が同じゲートウェイ上で設定されている必要があります。以下の設定により、SRST が音声ポートと MGCP ゲートウェイでの呼処理を制御することができます。Cisco IOS リリース 12.3(14)T でコマンド変更が行われたため、インストールした Cisco IOS リリースに対応する設定タスクを使用してください。



(注) 以下の設定で説明されているコマンドは、両方のコマンドが設定されていない限り有効ではありません。たとえば、**ccm-manager fallback-mgcp** コマンドを設定するだけでは設定は機能しません。



(注) MGCP が制御する PRI が SRST モードに切り替わった場合、ルータの NVRAM で設定を変更したり、変更を保存しないでください。SRST モードで設定が変更され、変更が保存されると、MGCP が通常動作に戻ったときに MGCP が制御する PRI に障害が発生します。

Cisco IOS リリース 12.3(14)T よりも前の MGCP ゲートウェイでの Cisco Unified SRST の設定

Cisco IOS リリース 12.3(14)T よりも前のソフトウェア リリースを使用している場合、MGCP ゲートウェイで Cisco Unified SRST をイネーブルにするには、このタスクを実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	<code>enable</code> 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	<code>configure terminal</code> 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	<code>ccm-manager fallback-mgcp</code> 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化し、Cisco Unified Communications Manager が使用できない場合に、MGCP 音声ゲートウェイが SRST または他の設定されたアプリケーションによって呼処理サービスを提供できるようにします。

コマンドまたはアクション	目的
<p>手順 4</p> <pre>call application alternate [application-name] or service [alternate default] service-name location</pre> <p>例:</p> <pre>Router(config)# call application alternate or Router(config)# service default</pre>	<p>call application alternate コマンドは、MGCP アプリケーションを利用できない場合に、デフォルトの音声アプリケーションが引き継ぐことを指定します。 <i>application-name</i> 引数はオプションであり、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を入力しないと、ゲートウェイはデフォルトのアプリケーションを使用します。</p> <p>または</p> <p>service コマンドは、特定のダイヤルピア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。次のキーワードと引数があります。</p> <ul style="list-style-type: none"> • alternate (任意)。ダイヤルピアにおいて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。 • default (任意)。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。 • <i>service-name</i>: 音声アプリケーションを特定する名前。 • <i>location</i>: URL 形式による、Tcl スクリプトまたは VoiceXML ドキュメントのディレクトリとファイル名。たとえば、フラッシュメモリ (flash:filename)、TFTP (tftp://./filename)、HTTP サーバ (http://./filename) などが有効な場所として指定できます。
<p>手順 5</p> <pre>exit</pre> <p>例:</p> <pre>Router(config)# exit</pre>	<p>グローバル 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 リリース 12.3(14)T 以降のリリースを使用した MGCP ゲートウェイでの Cisco Unified SRST の設定

Cisco IOS リリース 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 をイネーブルにするには、このタスクを実行します。

制約事項

Cisco IOS Release 12.3(14)T 以降、**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 リリース 12.3(14)T 以降のすべてのリリースで使用することができます。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
手順 1	enable 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	configure terminal 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	ccm-manager fallback-mgcp 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化し、Cisco Unified Communications Manager が使用できない場合に、MGCP 音声ゲートウェイが SRST または他の設定されたアプリケーションによって呼処理サービスを提供できるようにします。
手順 4	application [<i>application-name</i>] 例: Router(config) application app-xfer	<i>application-name</i> 引数はオプションであり、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を入力しないと、ゲートウェイはデフォルトのアプリケーションを使用します。
手順 5	global 例: Router(config)# global	グローバル 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
<p>手順 6 <code>service [alternate default] service-name location</code></p> <p>例: Router(config) service myapp https://myserver/myfile.vxml</p>	<p>特定のダイヤル ピアのスタンドアロン 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"> • alternate (任意)。ダイヤル ピアにおいて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。 • default (任意)。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。 • service-name: 音声アプリケーションを特定する名前。 • location: URL 形式による、Tel スクリプトまたは VoiceXML ドキュメントのディレクトリとファイル名。たとえば、フラッシュ メモリ (flash:filename)、TFTP (tftp://../filename)、HTTP サーバ (http://../filename) などが有効な場所として指定できます。
<p>手順 7 <code>exit</code></p> <p>例: Router(config)# exit</p>	<p>グローバル 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 リリース 12.3(14)T を使用した MGCP ゲートウェイで SRST をイネーブルにする設定例

以下に、Cisco IOS リリース 12.3(14)T 以降のリリースを使用している場合に、MGCP ゲートウェイで SRST を設定する例を示します。

```

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-l3 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 での DHCP の設定

このタスクを実行するには、ネットワークで DHCP が設定されている必要があります。DHCP の設定については、『[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 が Cisco Unified SRST システムに接続されている場合、自動的に DHCP サーバへの照会を行います。DHCP サーバは、IP アドレスを Cisco IP Phone に割り当て、DHCP オプション 150 を通じて TFTP サーバの IP アドレスを提供することで応答します。次に、電話機が Cisco Unified Communications Manager システム サーバに登録され、設定および電話機ファームウェアファイルを、DHCP サーバから提供される Cisco Unified Communications Manager TFTP サーバアドレスから取得します。

ネットワークの設定時に、お使いのサイトで DHCP サーバをローカルに設定します。SRST ルータを使用して DHCP サービスを提供することができます(推奨)。DHCP サーバが WAN 経由であり、WAN が長時間停止する場合、Cisco Unified IP Phone の DHCP リース時間が期限切れになる可能性があります。これにより、電話機が IP アドレスを使用できなくなり、結果的にサービスが失われます。DHCP リースの期限が切れた後で使用可能な DHCP サーバが存在しない場合、電話機を再起動しても電話機が再び動作することはありません。これは、電話機が IP アドレスなどの設定情報を取得できないためです。リモートサイトにローカルな DHCP サーバを設定しておくと、WAN に長時間の障害が発生した場合でも電話機が IP アドレスのリースを更新し続けることができます。

Cisco Unified IP Phone に DHCP サービスを設定するには、次のいずれかのタスクを選択してください。

- [単一の DHCP IP アドレス プールの定義 \(60 ページ\)](#): この方法は、Cisco Unified SRST ルータが DHCP サーバで、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。
- [Cisco Unified IP Phone ごとの個別の DHCP IP アドレス プールの定義 \(61 ページ\)](#): この方法は、Cisco Unified SRST ルータが DHCP サーバで、IP Phone 以外の DHCP クライアント用の別のプールが必要な場合に使用します。
- [DHCP リレー サーバの定義 \(62 ページ\)](#): 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 プールの定義

このタスクでは、すべての DHCP クライアントが同じ情報を受け取る、オプションの 150 TFTP サーバの IP アドレスを含めた、IP アドレスの大容量共有プールを作成します。この方法のメリットは、DHCP プールを 1 つだけ設定すればすむことです。ただし、単一の DHCP IP アドレス プールを定義することは、IP Phone 以外のクライアントが別の TFTP サーバアドレスを使用する必要がある場合、問題になる可能性があります。

手順の概要

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`

手順の詳細

	コマンドまたはアクション	目的
手順 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。
手順 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、スラッシュで始まるオプションのマスクまたはビット数を、アドレス プレフィックスで指定します。
手順 3	<code>option 150 ip ip-address</code> 例: Router(config-dhcp)# option 150 ip 10.0.22.1	Cisco IP Phone でイメージ コンフィギュレーション ファイルをダウンロードする TFTP サーバ アドレスを指定します。これは、Cisco Unified CM の IP アドレスである必要があります。
手順 4	<code>default-router ip-address</code> 例: Router(config-dhcp)# default-router 10.0.0.1	Cisco Unified IP Phone を直接接続する ルータを指定します。 <ul style="list-style-type: none"> このルータは、WAN 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であるため、Cisco Unified SRST ルータとしてください。Cisco IP Phone が Cisco Unified SRST ルータに接続されている限り、電話機は必要なネットワーク情報を取得できます。
手順 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。

Cisco Unified IP Phone ごとの個別の DHCP IP アドレス プールの定義

このタスクは 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。

手順の概要

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`

手順の詳細

	コマンドまたはアクション	目的
手順 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。
手順 2	<code>host ip-address subnet-mask</code> 例: Router(config-dhcp)# host 10.0.0.0 255.255.0.0	電話機が使用する IP アドレスを指定します。
手順 3	<code>option 150 ip ip-address</code> 例: Router(config-dhcp)# option 150 ip 10.0.22.1	Cisco IP Phone でイメージ コンフィギュレーション ファイルをダウンロードする TFTP サーバ アドレスを指定します。これは、Cisco Unified CM の IP アドレスである必要があります。
手順 4	<code>default-router ip-address</code> 例: Router(config-dhcp)# default-router 10.0.0.1	Cisco Unified IP Phone が直接接続するルータを指定します。 <ul style="list-style-type: none"> このルータは、WAN 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 アドレスであるため、Cisco Unified SRST ルータとしてください。Cisco IP Phone が Cisco Unified SRST ルータに接続されている限り、電話機は必要なネットワーク情報を取得できます。
手順 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 サーバの定義

このタスクでは、Cisco Unified IP Phone が接続されている LAN インターフェイスで DHCP リレーを設定し、Cisco IOS DHCP サーバ機能が DHCP クライアント(電話機)から DHCP サーバに要求をリレーできるようにします。DHCP の設定については、『[Cisco IOS DHCP Server](#)』を参照してください。

ルータでは、Cisco IOS DHCP サーバ機能はデフォルトでイネーブルになっています。DHCP サーバが Cisco Unified SRST ルータでイネーブルではない場合は、次の手順を使用してイネーブルにします。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	<code>service dhcp</code> 例: Router(config)# <code>service dhcp</code>	ルータで Cisco IOS DHCP サーバ機能をイネーブルにします。
手順 2	<code>interface type number</code> 例: Router(config)# <code>interface serial 0</code>	指定し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、『 Cisco IOS Interface and Hardware Component Command Reference, Release 12.3T 』を参照してください。
手順 3	<code>ip helper-address ip-address</code> 例: Router(config-if)# <code>ip helper-address 10.0.22.1</code>	認識できない TFTP サーバおよびドメイン ネーム システム (DNS) 要求のブロードキャスト用の、ヘルパー アドレスを指定します。各サーバで、サーバが異なるホストにある場合、サーバごとに別の <code>ip helper-address</code> コマンドが必要です。複数のサーバに <code>ip helper-address</code> コマンドを使用することで、複数の TFTP サーバターゲットを設定することもできます。
手順 4	<code>exit</code> 例: Router(config-if)# <code>exit</code>	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 インターバルとは、ネットワーク デバイスによって送信されるキープアライブ メッセージ同士の間隔です。キープアライブ メッセージとは、1 つのネットワーク デバイスからもう 1 つのネットワーク デバイスに対して、2 つのネットワーク デバイス間の仮想回線はまだアクティブであることを通知するために送信されるメッセージです。



(注) メッセージ間のデフォルトの間隔 (30 秒) を使用する計画であれば、このタスクを実行する必要はありません。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 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。
手順 2	<code>keepalive seconds</code> 例: Router(config-cm-fallback)# keepalive 60	Cisco Unified IP Phone によってルータに送信されるキープアライブ メッセージの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。
手順 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

次に、キープアライブ インターバルを 45 秒に設定する例を示します。

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

次の作業

次に、電話機を設定して、ダイヤル トーンを発生させます。手順については、以下を参照してください。[「Cisco Unified SIP SRST 4.1」セクション\(65 ページ\)](#)。

詳細については、「[Cisco Unified SRST 機能の概要](#)」セクション(1 ページ)の章の「[その他の関連資料](#)」セクション(28 ページ)を参照してください。



Cisco Unified SIP SRST 4.1

この章では、Cisco Unified SIP SRST 4.1 の機能を説明するとともに、構成情報を提供します。

- Out-Of-Dialog REFER (OOD-R)
- SIP 電話の桁収集
- 発信者 ID 表示
- コール自動転送およびコール転送の SIP 補足サービスのディセーブル化
- アイドルプロンプトステータス



(注) Cisco IOS リリース 12.4(15)T では、各プラットフォームでサポートされる SIP 電話の数は、サポートされる SCCP 電話の数と等しくなっています。たとえば、3845 は、SIP か SCCP かにかかわらず、720 台の電話機をサポートするようになっています。

目次

- [Cisco Unified SIP SRST 4.1 の前提条件 \(65 ページ\)](#)
- [Cisco Unified SIP SRST 4.1 の制約事項 \(66 ページ\)](#)
- [Cisco Unified SIP SRST 4.1 に関する情報 \(66 ページ\)](#)
- [Cisco Unified SIP SRST 4.1 機能の設定方法 \(69 ページ\)](#)
- [次の作業 \(73 ページ\)](#)

Cisco Unified SIP SRST 4.1 の前提条件

- Cisco IOS リリース 12.4(15)T 以降のリリース。
- Cisco Unified IP Phone 7911G、7941G、7941GE、7961G、7961GE、7970G、および 7971GE では、8.2(1) 以降のバージョンのファームウェアロードが必要です。
- バージョン 4.1 から導入された Cisco Unified SRST 機能の Enhanced 911 サービスの前提条件については、「[Prerequisites for Enhanced 911 Services](#)」を参照してください。

Cisco Unified SIP SRST 4.1 の制約事項

- Cisco Unified SRST は、BLF スピードダイヤル通知、不在転送の同期、ダイヤル プラン、ディレクトリ サービス、または保留音(MOH)をサポートしていません。
- SIP 電話ロード 8.0 より前では、SIP 電話は同時に Cisco Unified Communications Manager と Cisco Unified SRST の両方へのデュアル登録を維持していました。SIP 電話ロード 8.0 以降のバージョンでは、SIP 電話は、Cisco Unified Communications Manager への登録がアクティブな間、キープアライブを使用して、Cisco Unified SRST との接続を維持します。SIP 電話は、2 分ごとにキープアライブ メッセージを Cisco Unified SRST へ送信します。Cisco Unified SRST は、このキープアライブに 404 メッセージで応答します。このプロセスは、Cisco Unified SRST へのフォールバックが発生するまで繰り返されます。フォールバックの後、SIP 電話が Cisco Unified SRST に登録されている間、SIP 電話は 2 分ごとにキープアライブ メッセージを Cisco Unified Communications Manager に送信します。Cisco Unified SRST は、8.0 より前の SIP 電話ロードのデュアル登録を引き続きサポートします。

Cisco Unified SIP SRST 4.1 に関する情報

- [Out-Of-Dialog REFER \(66 ページ\)](#)
- [SIP 電話の桁収集 \(67 ページ\)](#)
- [発信者 ID 表示 \(68 ページ\)](#)
- [コール自動転送およびコール転送の SIP 補足サービスのディセーブル化 \(68 ページ\)](#)
- [アイドル プロンプト ステータス \(68 ページ\)](#)
- [Enhanced 911 サービス \(69 ページ\)](#)

Out-Of-Dialog REFER

Out-Of-Dialog REFER (OOD-R) によって、リモート アプリケーションは、最初の INVITE なしに REFER メッセージを Cisco Unified SRST に送信することでコールを確立できます。REFER が送信された後、コール セットアップの残りの部分はアプリケーションから独立し、メディア 스트リームはアプリケーションを通過しなくなります。OOD-R を使用するアプリケーションは、Request-URI で Referee アドレスを指定し、Refer-To ヘッダーで Refer-Target を指定するコール セットアップ要求をトリガーします。Cisco Unified SRST との通信に使用される SIP メッセージングは、エンドユーザのデバイス プロトコルに依存せず、H.323、単純な旧式の電話サービス (POTS)、SCCP、または SIP のいずれかになります。クリックツーダイヤルは、OOD-R を使用して作成できるアプリケーションの例です。

クリックツーダイヤル アプリケーションを使用すると、ユーザは、コール セットアップのための複数の手順を 1 回のクリックにまとめることができます。たとえば、ユーザは PC から Web ベースのディレクトリ アプリケーションをクリックすることで、電話番号を検索し、デスクトップ電話をオフフックにして、着信者番号をダイヤルできます。ユーザは自分の電話からダイヤルする必要なく、アプリケーションがコール セットアップを開始します。ディレクトリ アプリケーションが REFER メッセージを Cisco Unified SRST に送信し、Cisco Unified SRST がこの REFER に基づいて、両者の間のコールをセットアップします。

OOD-R の詳細については、『[Cisco Unified Communications Manager Express System Administrator Guide](#)』の「[Out-of-Dialog REFER](#)」を参照してください。

SIP 電話の桁収集

電話機ユーザによってダイヤルされた数字の文字列を収集して事前定義されたパターンと照合し、ユーザの入力に対応する宛先にコールを発信する必要があります。以前は、Cisco Unified SRST システム内の SIP 電話では、コール処理をトリガーするために、ユーザが Dial ソフト キーまたは # キーを押すか、桁間タイムアウトを待つ必要がありました。このため、コールの処理に遅延が発生することがありました。

SIP 電話では、電話のモデルに応じて、桁を収集および照合する 2 つの新しい方式がサポートされています。

- [KPML 桁収集 \(67 ページ\)](#)
- [SIP ダイヤル プラン \(67 ページ\)](#)

KPML 桁収集

Key Press Markup Language (KPML) は、SIP SUBSCRIBE および NOTIFY 方式を使用して、ユーザ入力を桁ごとに報告します。電話ユーザによってダイヤルされた各桁は、Cisco Unified SRST への独自のシグナリング メッセージを生成します。これにより、ダイヤルされた桁を収集するにつれ、接続先パターンをダイヤル ピアと照合することでパターン認識が実行されます。このプロセスでは、SCCP 電話機によって使用されるプロセスと同様に、各ディジットを即座にリレーします。これにより、桁が Cisco Unified SRST に送信されて処理される前に、ユーザが Dial ソフト キーを押したり、桁間タイムアウトを待機したりする必要がなくなります。

KPML は、Cisco Unified IP Phone 7911G、7941G、7941GE、7961G、7961GE、7970G、および 7971GE でサポートされています。設定については、「[SIP 電話の KPML の有効化](#)」セクション (69 ページ) を参照してください。

SIP ダイヤル プラン

ダイヤル プランは、ユーザがオフフックに移行して宛先番号にダイヤルした後、ディジット収集が完了したことを判断するために SIP Phone が使用するダイヤル パターンのセットです。ダイヤル プランにより、SIP 電話はローカルで桁収集を実行し、ユーザ入力が収集された際のダイヤル パターンを認識できます。パターンが認識された後、SIP 電話は Cisco Unified SRST に INVITE メッセージを送信し、ユーザの入力に一致する番号へのコールを開始します。ユーザによって入力されたすべての桁は、処理のためにブロックとして Cisco Unified SRST に提供されます。ディジット収集は電話機で行われるため、KPML ディジット収集と比較して、ダイヤル プランではシグナリング メッセージのオーバーヘッドが減少します。

SIP ダイヤル プランでは、発信 INVITE をトリガーするためにユーザが [ダイヤル (Dial)] ソフト キーまたは # キーを押すか、または桁間タイムアウトを待つ必要がなくなります。SIP ダイヤル プランを設定し、ダイヤル プランを SIP 電話機に関連付けます。ダイヤル プランはコンフィギュレーション ファイルで電話機にダウンロードされます。

SIP ダイヤル プランを設定し、それらを次の SIP 電話機に関連付けることができます。

- Cisco Unified IP Phone 7911G/7941G/7941GE/7961G/7961GE/7970G/7971GE: これらの電話はダイヤル プランを使用し、KPML をサポートします。ダイヤル プランと KPML の両方がイネーブルの場合は、ダイヤル プランが優先されます。
一致するダイヤル プランが見つからず、KPML が無効な場合、SIP NOTIFY メッセージが Cisco Unified SRST に送信されるまで、ユーザは桁間タイムアウトを待つ必要があります。その他の SIP 電話機とは異なり、オンフック ダイヤルを使用した場合を除き、これらの電話機にはダイヤルの終了を示す [ダイヤル (Dial)] ソフト キーがありません。

- Cisco Unified IP Phone 7905/7912/7940/7960: これらの電話はダイヤルプランを使用し、KPMLをサポートしません。これらの電話機に SIP ダイヤルプランを設定しない場合、またはダイヤルされた桁がダイヤルプランと一致しない場合は、桁が Cisco Unified SRST に送信され、処理される前に Dial ソフト キーを押すか、桁間タイムアウトを待つ必要があります。

電話機をリセットすると、電話機は TFTP サーバからコンフィギュレーション ファイルを要求し、電話機のタイプに基づいて適切なコンフィギュレーション ファイルが構築されます。

- Cisco Unified IP Phone 7905/7912: ダイヤルプランは、コンフィギュレーション ファイル内のフィールドです。
- Cisco Unified IP Phone 7911G/7940/7941G/7941GE/7960/7961G/7961GE/7970G/7971GE: ダイヤルプランは、通常のコンフィギュレーション ファイルから指される個別の XML ファイルです。

Cisco Unified SRST は、Cisco Unified Communications Manager でプロビジョニングされた場合は、SIP ダイヤルプランをサポートします。Cisco Unified SRST でダイヤルプランを設定することはできません。

発信者 ID 表示

Cisco Unified IP Phone 7911G、7941G、7941GE、7961G、7961GE、7970G、および 7971GE では、発信者の名前と番号がの発信者 ID の表示に含まれます。他の SIP 電話は発信者の番号のみが表示されます。また、発信者 ID 情報は、コール転送などの発信側の発信者 ID に変更が生じた場合、宛先の電話で更新されます。これらの拡張機能をサポートするために、新しい設定は必要ありません。

コール自動転送およびコール転送の SIP 補足サービスのディセーブル化

宛先ゲートウェイが補足サービスをサポートしていない場合、コール転送のための REFER メッセージおよび Cisco Unified SRST によって送信されたコール転送のためのリダイレクト応答を無効にすることができます。

すべてのエンドポイントが SCCP を使用している場合、またはすべてのエンドポイントが SIP を使用している場合の補足サービスの無効化がサポートされています。SCCP エンドポイントと SIP エンドポイントの混在はサポートされていません。

アイドルプロンプト ステータス

Cisco Unified SRST が Cisco Unified Communications Manager のフォールバックをサポートしていることを示すため、電話が Cisco Unified SRST に登録された後、SIP 電話のステータス行にメッセージが表示されます。このメッセージは、電話がフォールバック モードで動作しており、すべての機能が利用できるわけではないことをユーザに通知します。「CM フォールバック サービス動作中 (CM Fallback Service Operating)」を表示するデフォルトのメッセージは、電話のディクショナリ ファイルから取得されます。Cisco Unified SRST ルータで **system message** コマンドを使用して、メッセージをカスタマイズできます。Cisco Unified SRST は、SIP 電話が登録されるか、設定を通じてメッセージが変更された場合に、アイドルプロンプト メッセージを更新します。メッセージは、電話が Cisco Unified Communications Manager にスイッチバックするまで表示されます。

アイドルプロンプトステータスメッセージは、Cisco Unified SRST 4.1 以降のバージョンが導入された Cisco Unified IP Phone 7911G、7941G、7941GE、7961G、7961GE、7970G、7971GE でサポートされます。Cisco Unified SRST 4.1 より前のバージョンでは、電話はディクショナリファイルから取得したデフォルトのメッセージを表示します。

Enhanced 911 サービス

Cisco Unified SRST の Enhanced 911 サービスにより、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 発信者の位置を即時にピンポイントで検出する
- 切断された場合に、911 発信者にコールバックする

この機能が導入される前は、Cisco Unified SRST は 911 への発信コールのみをサポートしていました。基本 911 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 の 911 オペレータは、救急車サービス、消防署、警察署から対応チームが出動する前に、緊急情報と位置を発信者との会話によって収集する必要がありました。対応する特定の地理的な場所に基づいて、コールを異なる PSAP にルーティングすることはできませんでした。

Enhanced 911 サービスでは、発信者の位置に基づいて、911 コールは最も近い PSAP へ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自動的に PSAP の端末に表示されます。これにより、PSAP は発信者が位置を説明できない場合でも、緊急救助を迅速に派遣できます。さらに、発信者が途中で切断されると、PSAP には 911 発信者への連絡に必要な情報が提供されます。

詳細については、『[Cisco Unified Communications Manager Express System Administrator Guide](#)』の「[Configuring Enhanced 911 Services](#)」を参照してください。

Cisco Unified SIP SRST 4.1 機能の設定方法

ここでは、次の作業について説明します。

- [SIP 電話の KPML の有効化 \(69 ページ\)](#)
- [コール自動転送およびコール転送の SIP 補足サービスのディセーブル化 \(71 ページ\)](#)
- [SIP 電話のアイドルプロンプトステータスの設定 \(72 ページ\)](#)

SIP 電話の KPML の有効化

SIP 電話で KPML 桁収集を有効にするには、次の手順を実行します。

制約事項

- この機能は Cisco Unified IP Phone 7911G、7941GE、7941GE、7961G、7961GE、7970G、および 7971G-GE だけでサポートされます。
- 電話機に割り当てられたダイヤルプランは、KPML よりも優先されます。

手順の概要

1. `enable`
2. `configure terminal`
3. `voice register pool pool-tag`

4. `digit collect kpml`
5. `end`
6. `show voice register dial-peer`

手順の詳細

	コマンドまたはアクション	目的
手順 1	<code>enable</code> 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	<code>configure terminal</code> 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	<code>voice register pool pool-tag</code> 例: Router(config)# voice register pool 4	音声レジスタ プール コンフィギュレーション モードを開始して、SIP 電話機の電話機固有パラメータを設定します。 • <i>pool-tag</i> : 設定する SIP 電話の一意のシーケンス番号。範囲はバージョンとプラットフォームによって異なります。範囲を表示するには、 ? と入力します。 max-pool コマンドを使用すると、この引数の上限を変更できます。
手順 4	<code>digit collect kpml</code> 例: Router(config-register-pool)# digit collect kpml	SIP 電話機の KPML デジタル収集をイネーブルにします。 (注) このコマンドは、Cisco Unified CME および Cisco Unified SRST でサポートされている電話では、デフォルトで有効になっています。
手順 5	<code>end</code> 例: Router(config-register-pool)# end	特権 EXEC モードに戻ります。
手順 6	<code>show voice register dial-peers</code> 例: Router# show voice register dial-peers	定義された桁収集方法を含めて、Cisco Unified CME SIP レジスタに関連付けられた、動的に作成されたすべての VoIP ダイアル ピアの詳細を表示します。

次の作業

Cisco Unified SRST の KPML 設定を変更した後、新しい設定プロファイルを作成し、電話を再起動する必要はありません。KPML の有効化または無効化は、即座に Cisco Unified SRST に反映されます。

コール自動転送およびコール転送の SIP 補足サービスのディセーブル化

Cisco Unified SRST から接続先に送信される、コール転送用の REFER メッセージまたはコール転送用のリダイレクト応答を無効にするには、次の手順を実行します。宛先ゲートウェイでサポートされていない場合は、これらの補足サービス機能をディセーブルにできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice service voip**
または
dial-peer voice tag voip
4. **no supplementary-service sip {moved-temporarily | refer}**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
手順 1	enable 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	configure terminal 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	voice service voip または dial-peer voice tag voip 例: Router(config)# voice service voip または Router(config)# dial-peer voice 99 voip	音声サービス コンフィギュレーション モードを開始し、VoIP 機能のグローバル パラメータを設定します。 または ダイヤルピア コンフィギュレーション モードを開始して、特定のダイヤルピアに対するパラメータを設定します。

	コマンドまたはアクション	目的
手順 4	<pre>no supplementary-service sip {moved-temporarily refer} 例: Router(conf-voi-serv)# no supplementary-service sip refer または Router(config-dial-peer)# no supplementary-service sip refer</pre>	<p>SIP コール転送の補足サービスは、グローバルに無効にすることもできれば、1つのダイヤルピアに対して無効にすることもできます。</p> <ul style="list-style-type: none"> • moved-temporarily: コール転送用の SIP リダイレクト応答。 • refer: コール転送用の SIP REFER メッセージ。 • 接続先へ REFER メッセージおよびリダイレクトメッセージを送信するのがデフォルト動作です。 <p>(注) このコマンドは、SIP 電話間のコールと SCCP 電話間のコールに対してサポートされています。SCCP エンドポイントと SIP エンドポイントの混在はサポートされていません。</p>
手順 5	<pre>end 例: Router(config-voi-serv)# end または Router(config-dial-peer)# end</pre>	特権 EXEC モードに戻ります。

SIP 電話のアイドルプロンプトステータスの設定

SIP 電話が Cisco Unified SRST へフェールオーバーした後に、SIP 電話に表示するメッセージをカスタマイズするには、次の手順を実行します。



(注)

Cisco Unified SRST でアイドルステータスメッセージを変更した後に、**create profile** コマンドを使用して新しい設定ファイルを作成し、電話を再起動する必要はありません。ステータスメッセージの変更は、即座に Cisco Unified SRST に反映されます。

前提条件

Cisco Unified SRST 4.1 以降のバージョン。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **system message *string***
5. **end**
6. **show voice register global**

手順の詳細

	コマンドまたはアクション	目的
手順 1	<code>enable</code> 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	<code>configure terminal</code> 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	<code>voice register global</code> 例: Router(config)# voice register global	音声レジスタ グローバル コンフィギュレーション モードを開始して、Cisco Unified CME 環境でサポートされるすべての SIP 電話機に対してグローバル パラメータを設定します。
手順 4	<code>system message string</code> 例: Router(config-register-global)# system message fallback active	Cisco Unified SRST に登録されている SIP 電話で表示するステータス メッセージを定義します。 • <i>string</i> : 最大 32 文字の英数字。デフォルトは「CM フォールバック サービス動作中 (CM Fallback Service Operating)」です。
手順 5	<code>end</code> 例: Router(config-register-global)# end	特権 EXEC モードに戻ります。
手順 6	<code>show voice register global</code> 例: Router# show voice register global	SIP 電話に関連付けられたすべてのグローバル コンフィギュレーション パラメータを表示します。

次の作業

次の作業では、SCCP を使用して Cisco Unified IP Phone を設定します。手順については、「[SCCP を用いた Cisco Unified IP Phone の設定](#)」セクション(75 ページ)を参照してください。

詳細については、「[Cisco Unified SRST 機能の概要](#)」セクション(1 ページ)の章の「[その他の関連資料](#)」セクション(28 ページ)を参照してください。

■ 次の作業



SCCP を用いた Cisco Unified IP Phone の設定

この章では、Cisco Unified CM のフォールバックの間に Cisco Unified IP Phone に表示されるディスプレイと発信者が使用する機能を設定する方法を説明します。



(注) この章で説明する Cisco Unified IP Phone は単なる例を示しています。IP Phone の完全なリストについては、[Compatibility Information](#) を参照してください。

目次

- [Cisco Unified IP Phone の設定に関する情報\(75 ページ\)](#)
- [Cisco Unified IP Phone の設定方法\(76 ページ\)](#)
- [Cisco Unified SRST 向けの Cisco IP Communicator の設定方法\(91 ページ\)](#)
- [次の作業\(92 ページ\)](#)

Cisco Unified IP Phone の設定に関する情報

Cisco Unified SRST では Cisco Unified IP Phone の設定が制限されています。その理由は、Cisco Unified CM のフォールバックの間に IP Phone はほぼすべての Cisco Unified CM の設定を保持するためです。Cisco Unified Communications Manager のフォールバックの間に Cisco Unified IP Phone に表示される日付形式、時間形式、言語、およびシステム メッセージを設定することができます。これら 4 つの設定すべてにデフォルト値があり、利用可能な言語のオプションは使用中の IP Phone と Cisco Unified CM のバージョンによって異なります。また、設定では 2 次ダイヤルトーンを使用できます。これは、電話機のユーザが事前定義 PSTN アクセス プレフィックスをダイヤルしたときに生成され、追加の番号をダイヤルしたときに終了することができます。二重回線の電話設定は、Cisco Unified CM のフォールバックの間に二重回線の電話操作をするために必要となります。

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。

- 電話機能をサポートするための Cisco Unified SRST の設定 (76 ページ) (必須)
- Cisco Unified 8941 および 8945 SCCP IP Phone の設定 (78 ページ) (必須)
- Cisco Unified SRST がイネーブルであることの確認 (79 ページ) (任意)
- IP Phone の時計、日付、時刻形式の設定 (80 ページ) (任意)
- IP Phone の言語表示の設定 (82 ページ) (任意)
- Cisco Unified IP Phone 用にカスタマイズしたシステム メッセージの設定 (83 ページ) (任意)
- 2 次ダイヤル トーンの設定 (84 ページ) (任意)
- 二重回線の電話設定 (85 ページ) (特定の条件下で必要)
- 各ボタンで 8 つのコールの設定 (オクトライン) (87 ページ) (任意)
- コールの最大数の設定 (89 ページ) (任意)
- トラブルシューティング (90 ページ) (任意)

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 がイネーブルであれば、Cisco Unified Communications Manager のフォールバック モードの間に Cisco Unified IP Phone を再設定する必要はありません。これは、すべての電話機が Cisco Unified Communications Manager で使用したのと同じ設定を保持するためです。

Cisco Unified IP Phone 機能をサポートするようにルータ上で Cisco Unified SRST を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

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** *phone-type max-lines*
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
手順 1	<p>call-manager-fallback</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>
手順 2	<p>ip source-address ip-address [port port] [any-match strict-match]</p> <p>例: Router(config-cm-fallback)# ip source-address 10.6.21.4 port 2002 strict-match</p>	<p>ルータが Cisco IP Phone から指定した IP アドレスによってメッセージを受信できるようにし、厳密な IP アドレス確認を提供します。デフォルトのポート番号は 2000 です。</p>
手順 3	<p>max-dn max-directory-numbers [dual-line] [preference preference-order]</p> <p>例: Router(config-cm-fallback)# max-dn 15 dual-line preference 1</p>	<p>ルータがサポートできる最大数の電話番号(DN)または仮想音声ポートを設定し、二重回線モードを作動させます。</p> <ul style="list-style-type: none"> • max-directory-numbers:ルータがサポートできる最大数の電話番号(DN)または仮想音声ポート。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、Compatibility Information を参照してください。 • dual-line(任意)。Cisco Unified Communications Manager のフォールバック モードで、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。 • preference preference-order(任意)。プライマリ番号に関連付けられているすべての電話番号に VoIP ダイアルピアを作成するためのグローバル設定を設定します。範囲は 0 ~ 10 です。デフォルトは 0 です。これが最も高いプリファレンスです。 <p>alias コマンドは、alias コマンドの設定値を指定する preference キーワードを使用できます。alias コマンドの preference キーワードを設定すると、max-dn コマンドで設定されたデフォルト設定をオーバーライドすることができます。max-dn コマンドを alias コマンドで使用方法については、「コール再ルーティングの設定」セクション(115 ページ)を参照してください。</p> <p>(注) 最大数の番号を設定したら、電話番号または仮想音声ポートの制限を減らすためにルータの再起動が必要です。</p>

	コマンドまたはアクション	目的
手順 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、Compatibility Information を参照してください。</p> <p>(注) 最大数の番号を設定したら、Cisco IP Phone の制限を減らすためにルータの再起動が必要です。</p>
手順 5	<p><code>limit-dn phone-type max-lines</code></p> <p>例: Router(config-cm-fallback)# limit-dn 7945 2</p>	<p>(任意) Cisco Unified CM のフォールバックの間の 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、Cisco Unified SRST ルータの初回設定の間に、電話機が実際に Cisco Unified SRST ルータに登録される前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>使用できる電話機のリストについては、『Cisco SRST and SIP SRST Command Reference (All Versions)』を参照してください。</p> <p>回線の最大数は、1 ~ 6 の範囲で指定します。電話番号の最大数のデフォルト値は 6 に設定されています。最後の回線番号がこの制限を超えているアクティブな電話がある場合、電話機をリセットするように警告する情報が表示されます。</p>
手順 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 8941 および 8945 SCCP IP Phone の設定

Cisco Unified 8941/8945 SCCP IP Phone を SRST モードで設定するには、以下のコマンドを実行します。



(注) このセクションは SRST バージョン 8.6 に限り必要であり、バージョン 8.6 以降では必要ではありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ephone-type** *phone-type*
4. **device-id** *number*
5. **device-type** *phone-type*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
手順 1	enable 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	configure terminal 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	ephone-type <i>phone-type</i> 例: Router(config)# ephone-type 8941	設定する電話機のタイプを入力します。 • 8941 • 8945
手順 4	device-id <i>number</i> 例: Router(config-ephone-type)# device-id 586	電話機タイプのデバイス ID を指定します。 • 8941—586 • 8945—585
手順 5	device-type <i>phone-type</i> 例: Router(config-ephone-type)# device-type 8941	電話機のデバイス タイプを指定します。 • 8941 • 8945
手順 6	end 例: Router(config-ephone-type)# end	特権 EXEC モードに戻ります。

Cisco Unified SRST がイネーブルであることの確認

Cisco Unified SRST 機能がイネーブルであることを確認するには、次の手順を実行します。

- 手順 1 **show running-config** コマンドを入力して、設定を確認します。
- 手順 2 **show call-manager-fallback all** コマンドを入力し、Cisco Unified SRST 機能がイネーブルになっていることを確認します。
- 手順 3 ネットワーク内の Cisco IP Phone の設定ディスプレイを使用して、電話機のデフォルト 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します。

- 手順 4 Cisco IP Phone 1 台の TCP ポート 2000 Skinny Client Control Protocol (SCCP) 接続を一時的にブロックし、Cisco IP Phone が Cisco Unified Communications Manager に接続しないようにして Cisco Unified SRST ルータに登録するには、次の手順を実行します。
- a. Cisco Unified IP Phone を Cisco Unified Communications Manager から一時的に切断するには、適切な **IP access-list** コマンドを使用します。
WAN 接続に障害が発生した場合、Cisco Unified SRST がイネーブルになっていると、Cisco Unified Communications Manager のフォールバック モードで実行されていることを通知するメッセージが Cisco Unified IP Phone に表示されます。Cisco Unified Communications Manager のフォールバック モードで動作している場合、Cisco IP Phone 7960 および Cisco IP Phone 7940 では「CM フォールバック サービスが実行中 (CM Fallback Service Operating)」というメッセージが表示され、Cisco IP Phone 7910 では「CM フォールバック サービス (CM Fallback Service)」というメッセージが表示されます。Cisco Unified Communications Manager が復元されると、このメッセージは消え、Cisco IP Phone の機能が完全に復元されます。
 - b. Cisco Unified SRST ルータでの Cisco IP Phone の登録プロセスを確認するには、**debug ephone register** コマンドを使用します。
 - c. Cisco Unified SRST ルータに登録されている Cisco IP Phone を表示するには、**show ephone** コマンドを使用します。
 - d. 電話機の通常のサービスに戻るには、適切な **access-list** コマンドの **no** 形式を使用します。

IP Phone の時計、日付、時刻形式の設定

Cisco Unified IP Phone 7970G および Cisco Unified IP Phone 7971G-GE IP Phone は、正しいタイムゾーンを Cisco Unified Communications Manager から取得します。さらに、SRST の登録時に SRST ルータから協定世界時 (UTC) 時刻を受信します。SRST モードの間に電話機はタイムゾーンと UTC 時刻を取得し、タイムゾーンにオフセットを適用して正しい時刻を表示させます。

Cisco IP Phone 7960 IP Phone や、Cisco IP Phone 7940 などの SCCP 電話機は、SRST の登録時に SRST ルータのローカル時間からディスプレイ時刻情報を取得します。Cisco Unified SRST ルータが Network Time Protocol (NTP) を使用して NTP タイムサーバから Cisco Unified SRST ルータの時刻を自動的に同期するように設定されている場合、UTC 時刻だけがルータに送られます。これは、NTP サーバが物理的に世界中のあらゆる場所、あらゆるタイムゾーンに設置されている可能性があるためです。正しい現地時間を表示することが重要ですので、**clock timezone** コマンドを使用して Cisco Unified SRST ルータの時刻を調整またはオフセットします。

Cisco Unified CM のフォールバック モードですべての Cisco Unified IP Phone のディスプレイに表示される日付と時間は、次の設定のように **date-format** および **time-format** コマンドを使用して選択されます。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
手順 1	<pre>clock timezone zone hours-offset [minutes-offset]</pre> <p>例: Router(config)# clock timezone PST -8</p>	<p>表示のためのタイムゾーンを設定します。</p> <ul style="list-style-type: none"> • <i>zone</i>: 標準時が適用されているときに表示されるタイムゾーンの名前。<i>zone</i> 引数の最大長は、7 文字に制限されています。 • <i>hours-offset</i>: 協定世界時(UTC)からの時差。 • <i>minutes-offset</i>(任意): UTC からの分単位の差。
手順 2	<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>
手順 3	<pre>date-format {mm-dd-yy dd-mm-yy yy-dd-mm yy-mm-dd}</pre> <p>例: Router(config-cm-fallback)# date-format yy-dd-mm</p>	<p>IP Phone ディスプレイの日付の表示形式を設定します。選択肢は、mm-dd-yy、dd-mm-yy、yy-dd-mm、および yy-mm-dd です。</p> <ul style="list-style-type: none"> • dd: 日 • mm: 月 • yy: 年 <p>デフォルトでは mm-dd-yy に設定されます。</p>
手順 4	<pre>time-format {12 24}</pre> <p>例: Router(config-cm-fallback)# time-format 24</p>	<p>ルータに登録されているすべての Cisco Unified IP Phone の時刻の表示形式を設定します。デフォルトでは 12 時間表示に設定されます。</p>
手順 5	<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

次に、タイムゾーンを太平洋標準時間(PST)(UTC からマイナス 8 時間)に設定し、時刻の表示形式を 24 時間表示に設定する例を示します。

```
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 CM のフォールバックの間に Cisco Unified IP Phone で表示される言語は、デフォルトで US (米国) の ISO-3166 国別コードに設定されています。The Cisco Unified IP Phone 7940 および Cisco Unified IP Phone 7960 は、**user-locale** コマンドを使用してさまざまな言語 (文字セットやつづりのルール) を設定できます。



(注)

この設定オプションは、Cisco Unified CM V3.2 以降のバージョンで実行されている Cisco SRST V2.1 以降のバージョンで利用できます。システムが Cisco Unified SRST V2.1 と Cisco Unified CM V3.2 より前のソフトウェアを搭載している場合、デフォルトの国である米国 (US) のみを使用できます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 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。
手順 2	user-locale <i>country-code</i> 例: Router(config-cm-fallback)# user-locale ES	Cisco IP Phone 7940 および Cisco IP Phone 7960 のディスプレイに使用する国別の言語を選択します。 Cisco Communications Manager V3.2 以降のバージョンを実行している Cisco SRST および Cisco Unified SRST システムでは、次の ISO-3166 コードを使用できます。 <ul style="list-style-type: none"> • DE: ドイツ語 • DK: デンマーク語 • ES: スペイン語 • FR: フランス語 • IT: イタリア語 • JP: 日本語カタカナ (Cisco Unified Communications Manager V4.0 以降のバージョンで使用可能) • NL: オランダ語 • NO: ノルウェー語 • PT: ポルトガル語 • RU: ロシア語 • SE: スウェーデン語 • US: 米国英語 (デフォルト)
手順 3	exit 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

次に、ポルトガルのユーザ ロケールの設定例を示します。

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

Cisco Unified IP Phone 用にカスタマイズしたシステムメッセージの設定

Cisco Unified CM のフォールバックの間にすべての Cisco Unified IP Phone に表示されるシステムメッセージをカスタマイズするには、**system message** コマンドを使用します。

primary と **secondary** の 2 つのキーワードのいずれかをコマンドに含める必要があります。

primary キーワードは、フォールバック中の静的テキストメッセージをサポートする IP Phone 用です。フォールバック モードでプライマリ IP Phone にデフォルトで表示されるメッセージは、「CM フォールバック サービスが実行中 (CM Fallback Service Operating)」です。

secondary キーワードは、静的テキストメッセージをサポートせず、表示スペースが限られている Cisco Unified IP Phone 向けです。セカンダリ IP Phone はフォールバック中にメッセージをフラッシュします。フォールバック モードでセカンダリ IP Phone にデフォルトで表示されるメッセージは、「CM フォールバック サービス (CM Fallback Service)」です。

表示メッセージの変更は、設定の直後、または各コールの終了時に起こります。



(注)

正常なインサービス静的テキストメッセージは Cisco Unified Communications Manager によって制御されます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 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。
手順 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 モードでの IP Phone 上の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"> • primary primary-string: Cisco Unified IP Phone 7940 および Cisco Unified IP Phone 7960 ユニットなど、フォールバック中に静的テキストメッセージをサポートする Cisco Unified IP Phone 向け。約 27 ~ 30 文字の文字列を使用できます。 • secondary secondary-string: Cisco Unified IP Phone 7910 など、静的テキストメッセージをサポートしない Cisco Unified IP Phone 向け。約 20 文字の文字列を使用できます。
手順 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

次に、ルータ上のすべての Cisco Unified IP Phone でシステム表示メッセージとして「SRST V3.0」を設定する例を示します。

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

2 次ダイヤル トーンの設定

2 次ダイヤル トーンは、電話機のユーザが事前定義 PSTN アクセス プレフィックスをダイヤルしたときに生成され、追加の番号をダイヤルしたときに終了することができます。たとえば、外部回線に接続するために番号 9 をダイヤルした後に、2 次ダイヤル トーンが聞こえます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 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。
手順 2	<code>secondary-dialtone digit-string</code> 例: Router(config-cm-fallback)# secondary-dialtone 9	digit-string がダイヤルされたときに、2 次ダイヤル トーンをアクティブにします。
手順 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

次に、2 次ダイヤル トーンをトリガーするために番号 8 を設定する例を示します。

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

二重回線の電話設定

二重回線の電話設定は、Cisco Unified CM のフォールバックの間に二重回線の電話操作をするために必要となります。「Cisco SRST 3.0 で H.450.2 および H.450.3 を使用したコンサルタティブ コールの転送および自動転送の有効化」セクション(133 ページ)を参照してください。

二重回線 IP Phone は、Cisco Unified CM のフォールバック中に `max-dn` コマンドを使用してサポートされます。二重回線 IP Phone には、独立した 2 つのコールを処理するための 2 つのチャンネルを持つ 1 つの音声ポートがあります。この機能は、電話回線ボタン上のコール待機、コール転送、および電話会議機能を有効にします。

二重回線モードでは、各 IP Phone およびそれに関連付けられている回線ボタンが 1 ~ 2 つのコールをサポートできます。同一回線にある 2 つのコールのうちどちらを選択するかは、電話機のディスプレイの下にある青いナビゲーション ボタンを使用して決定します。二重回線チャンネルの 1 つが特定の電話で使用されているとき、`ephone-dn` を共有する他の電話機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ています。

セカンダリ チャンネルではハンティングを無効にすることが推奨されます。詳細については、「ダイヤルピア チャンネル ハントの設定」セクション(130 ページ)を参照してください。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 例: <pre>Router(config)# call-manager-fallback</pre>	call-manager-fallback コンフィギュレーション モードを開始します。
手順 2	max-dn max-directory-numbers [dual-line] [preference preference-order] 例: <pre>Router(config-cm-fallback)# max-dn 15 dual-line preference 1</pre>	ルータがサポートできる最大数の電話番号(DN)または仮想音声ポートを設定し、二重回線モードを作動させます。 <ul style="list-style-type: none"> • max-directory-numbers: ルータがサポートできる最大数の電話番号 (DN) または仮想音声ポート。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、Compatibility Information を参照してください。 • dual-line (任意)。Cisco Unified Communications Manager のフォールバック モードで、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。 • preference preference-order (任意)。プライマリ番号に関連付けられているすべての電話番号に VoIP ダイヤルピアを作成するためのグローバル設定を設定します。範囲は 0 ~ 10 です。デフォルトは 0 です。これが最も高いプリファレンスです。 alias コマンドは、alias コマンドの設定値を指定する preference キーワードを使用できます。alias コマンドの preference キーワードを設定すると、max-dn コマンドで設定されたデフォルト設定をオーバーライドすることができます。max-dn コマンドを alias コマンドで使用する方法については、「コール再ルーティングの設定」セクション (115 ページ) を参照してください。
手順 3	exit 例: <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。

例

次に、ルータがサポートできる最大数の DN または仮想音声ポートを 10 に設定し、Cisco Unified CM フォールバック モードのすべての IP Phone で二重回線モードを作動させる例を示します。

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

各ボタンで 8 つのコールの設定(オクトライン)

オクトライン機能は、単一のボタンで最大 8 つのアクティブ コール(着信と発信の両方)をサポートします。オクトラインの電話番号に 8 つの着信コールがあると、8 つの呼出音が同時に鳴ります。1 つの着信コールに应答するとその呼出音は止み、残りの 7 つの着信コールにはコール ウェイティング トーンが鳴ります。

オクトラインの電話番号への着信コールに应答した後、应答側の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。後続の着信コールは、コールに接続された電話にコール ウェイティング トーンを送信し、**remoteMultiline** 状態に入っている他の電話に呼出音を送信します。電話番号を共有するすべての電話機は、应答されていない任意の着信コールを受けることができます。

複数の電話間で共有されるオクトラインの電話番号で複数の着信コールが呼び出されている場合、コールに应答した電話機では呼出音が停止し、他の应答されていないコールではコール ウェイティング トーンが聞こえます。呼び出し中のコールの複数のインスタンスは、電話番号を共有する他の **ephone** 上に表示されます。オクトラインのディレクトリ番号で接続したコールを保留状態にすると、このディレクトリ番号を共有するどの電話機でも、保留中のコールに应答できます。電話機がコール転送中または電話会議を作成しているとき、そのオクトラインの電話番号を共有する他の電話機でそのコールを聞くことはできません。

オクトラインで新しいコールを着信すると、システムは、**huntstop chan tag** コマンドを使用して、次に使用可能なアイドル回線を探します。**tag** は 1 から 8 までの番号です。アイドルチャンネルは最小値から最大値まで選択されます。最大数の可能なコールを受信すると、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。オクトラインの電話番号に着信するコール数を制限したり、発信コールまたはコールの転送や電話会議などの機能用にチャンネルを予約するには、次のコマンドを使用します。

新しい機能では、次の操作を実行できます。

- 二重回線モードのみの設定
- オクトライン モードのみの設定
- 二重回線モードとオクトライン モードの設定

前提条件

- Cisco Unified SRST 7.0/4.3
- Cisco Unified CM 6.0
- Cisco IOS Release 12.4(15)XZ

制約事項

オクトラインの電話番号は、Cisco ATA または Cisco VG224 に接続された Cisco Unified IP Phone 7902、7920、7931、またはアナログ電話機ではサポートされていません。

手順の概要

1. **enable**
2. **configure terminal**
3. **call-manager-fallback**
4. **max-dn max-no-of-directories [dual-line | octo-line] [number octo-line]**

5. huntstop channel 1-8

6. end

手順の詳細

	コマンドまたはアクション	目的
手順 1	<code>enable</code> 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	<code>configure terminal</code> 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	<code>call-manager-fallback</code> 例: Router(config)# call-manager-fallback	<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。
手順 4	<code>max-dn max-no-of-directories [dual-line octo-line] [number octo-line]</code> 例: Router(config-cm-fallback)# max-dn 15 dual-line 6 octo-line	ルータがサポートできる最大数の DN または仮想音声ポートを設定し、二重回線モード、オクトラインモード、または両方のモードを作動させます。 • max-no-of-directories : ルータがサポートできる最大数の電話番号 (DN) または仮想音声ポート。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 : (任意) Cisco Unified Communications Manager のフォールバック モードで、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 : (任意) Cisco Unified Communications Manager のフォールバック モードで、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。 • number : (任意) オクトモードの電話番号の数を設定します。
手順 5	<code>huntstop channel 1-8</code> 例: Router(config-cm-fallback)# huntstop channel 4	オクトラインでのチャネルハントストップを有効にします。チャネルハントストップにより、最後の可能なチャネルが話中か応答しない場合に、電話回線の次のチャネルをハントしなくなります。 • number : 着信コールの受け入れに使用可能なチャネル数。残りのチャネルは、発信コールと、コール転送、コール待機、および電話会議などの機能に予約されます。指定できる範囲は 1 ~ 8 であり、デフォルトは 8 に設定されています。 • コマンドは、オクトラインの電話番号でのみサポートされています。
手順 6	<code>end</code> 例: Router(config)# end	特権 EXEC モードに戻ります。

例

次の例では、オクトラインモードが有効であり、8つのオクトラインの電話番号と最大23の電話番号があり、最大6つのチャンネルを着信コールに使用できます。

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

コールの最大数の設定

Cisco Unified SRST 9.0 の Cisco Unified SCCP IP Phone でコールの最大数を設定するには、次の手順を実行します。

前提条件

- Cisco SRST 9.0 以降のバージョン。
- 9.2(1) 以降のバージョンの正しいファームウェアがインストールされていること。

手順の概要

1. **enable**
2. **configure terminal**
3. **call-manager-fallback**
4. **max-dn max-no-of-directories [dual-line | octo-line]**
5. **timeouts busy seconds**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
手順 1	enable 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	configure terminal 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	call-manager-fallback 例: Router(config)# call-manager-fallback	Cisco Unified SRST サポートをイネーブルにして、 call-manager-fallback 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
手順 4	<p><code>max-dn max-no-of-directories [dual-line octo-line]</code></p> <p>例: Router(config-cm-fallback)# max-dn 10 octo-line</p>	<p>ルータがサポートできる最大数の電話番号または仮想音声ポートを設定し、二重回線モード、オクトラインモード、または両方のモードを作動させます。</p> <ul style="list-style-type: none"> • max-no-of-directories: ルータがサポートできる最大数の電話番号または仮想音声ポート。最大数はプラットフォームによって異なります。デフォルトは仮想ポートあたり電話番号は 0 でチャンネルは 1 つです。 • dual-line: (任意) Cisco Unified SRST ルータに接続されているすべての Cisco Unified IP Phone が、2 つのチャンネルを持つ仮想音声ポートを使用するように設定します。 • octo-line: (任意) Cisco Unified SRST ルータに接続されているすべての Cisco Unified IP Phone が、8 つのチャンネルを持つ仮想音声ポートを使用するように設定します。
手順 5	<p><code>timeouts busy seconds</code></p> <p>例: Router(config-cm-fallback)# timeouts busy 10</p>	<p>話中の宛先へのコール転送のタイムアウト値を設定します。</p> <ul style="list-style-type: none"> • seconds: 話中の宛先へ接続してから転送コールが切断されるまでの秒数。範囲は 0 ~ 30 です。デフォルト: 10。
手順 6	<p><code>end</code></p> <p>例: Router(config-cm-fallback)# end</p>	<p>コンフィギュレーションモードを終了して、特権 EXEC モードを開始します。</p>

トラブルシューティング

Cisco Unified SRST の設定に関して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 のキープアライブ 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 の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 の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 の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 のエラー 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 のコール統計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提供し、1024 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 メッセージで生の低レベル 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 Debug Command Reference](#)』を参照してください。

Cisco Unified SRST 向けの Cisco IP Communicator の設定方法

Cisco IP Communicator は、拡張テレフォニー サポートをパーソナル コンピュータ経由で配信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、ソフトキーを備えたグラフィカルなディスプレイベースの IP Phone としてユーザのコンピュータ モニタに表示されます。

操作については、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、以下が必要です。

- Cisco Unified CM (Call Manager) TFTP サーバの IP アドレス
- Cisco Unified SRST TFTP サーバの IP アドレス
- PC 用のマイク付きヘッドセット (任意。PC の内蔵のスピーカーとマイクを使用できます)

-
- 手順 1** Cisco IP Communicator ソフトウェアの最新バージョンをダウンロードして、PC にインストールします。このソフトウェアは、<http://www.cisco.com/cisco/web/download/index.html> からダウンロードできます。
- a. [音声およびユニファイド コミュニケーション (Voice and Unified Communication)] をクリックします。
 - b. [IP テレフォニー (IP Telephony)] をクリックします。
 - c. [IP フォン (IP Phones)] をクリックします。
 - d. [Cisco IP Communicator] をクリックします。
- 手順 2** (任意) PC にヘッドセットを接続します。
- 手順 3** Cisco IP Communicator ソフトウェア アプリケーションを起動します。
- 手順 4** Cisco Unified CM の IP アドレスをプライマリ TFTP サーバとして定義します。
- a. [ネットワーク (Network)] > [ユーザ プリファレンス (User Preferences)] ウィンドウを開きます。
 - b. Cisco Unified CM TFTP サーバの IP アドレスを入力します。
- 手順 5** Cisco Unified SRST の IP アドレスをセカンダリ TFTP サーバとして定義します。
- a. [ネットワーク (Network)] > [ユーザ プリファレンス (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。
- 手順 6** Cisco IP Communicator が少なくとも 1 度は Cisco Unified CM に登録されていることを確認します。詳細については、『*Install and Configure IP Communicator with CallManager*』を参照してください。
- 手順 7** Cisco IP Communicator が Cisco Unified SRST システムに接続し (Cisco Unified CM に障害が発生した場合など)、自身を登録するまで待ちます。
- 手順 8** Cisco IP Communicator は、Cisco IP Communicator の元のボタンと数を維持しています。
-

Cisco IP Communicator の確認

-
- 手順 1 この電話機に関連付けられた ephone-dn および ephone の情報を表示するには、**show running-config** コマンドを使用します。
 - 手順 2 Cisco IP Communicator は、Cisco Unified SRST に登録された後、設定に電話機の内線とソフトキーを表示します。これらが正しいことを確認します。
 - 手順 3 この電話機からのローカル コールの発信、および任意の相手からのコールの受信を行います。双方向音声パスを確認します。
-

Cisco IP Communicator のトラブルシューティング

コールの問題を診断するには、**debug ephone detail** コマンドを使用します。詳細については、『[Cisco IOS Debug Command Reference](#)』を参照してください。

次の作業

次に、SIP を使用して Cisco Unified IP Phone を設定します。詳細については、『[SIP を用いた Cisco Unified IP Phone の設定](#)」セクション(93 ページ)を参照してください。

詳細については、『[その他の関連資料](#)」セクション(28 ページ)を参照してください。



SIP を用いた Cisco Unified IP Phone の設定

Cisco IOS ソフトウェアにおける Session Initiation Protocol (SIP) レジストラ機能は、Cisco Unified SIP Survivable Remote Site Telephony (SRST) にとって非常に重要な要素です。SIP レジストラは RFC 3261 に従って登録要求を受け入れるサーバであり、通常はプロキシまたはリダイレクトサーバと同じ場所に配置されます。SIP レジストラは、ロケーション サービスも提供します。

目次

- [SIP レジストラを設定するための前提条件 \(93 ページ\)](#)
- [SIP レジストラの設定に関する制約事項 \(93 ページ\)](#)
- [SIP レジストラの設定に関する情報 \(93 ページ\)](#)
- [SIP レジストラの設定方法 \(94 ページ\)](#)
- [次の作業 \(107 ページ\)](#)

SIP レジストラを設定するための前提条件

[「Cisco Unified SRST 機能の概要」セクション \(1 ページ\)](#) の [「Cisco Unified SIP SRST を設定するための前提条件」セクション \(9 ページ\)](#) セクションに記載された前提条件を満たす必要があります。

SIP レジストラの設定に関する制約事項

[「Cisco Unified SRST 機能の概要」セクション \(1 ページ\)](#) の [「Cisco Unified SIP SRST の設定に関する制約事項」セクション \(10 ページ\)](#) セクションに記載された制約事項を参照してください。

SIP レジストラの設定に関する情報

Cisco Unified SIP SRST は、基本レジストラとコール処理サービスの提供により、外部 SIP プロキシサーバにバックアップを提供します。これらのサービスは、WAN 接続に障害が発生し、SIP 電話がプライマリ SIP プロキシと通信できない場合に SIP IP Phone で使用されます。Cisco Unified SIP SRST のデバイスは、PSTN コールの発信と着信のために PSTN ゲートウェイ アクセスを提供します。

Cisco Unified SIP SRST は、次のタイプの発信で機能します。

- 主要なプロキシが使用できない場合、ローカル SIP IP Phone からローカル SIP 電話への発信。
- ローカル SIP IP Phone から発信 PSTN への制限クラス (COR) などの追加サービス。たとえば、1 ~ 900 番の発信をブロックするため。

SIP レジストラの設定方法

ここでは、次の手順について説明します。

- [SIP レジストラの設定 \(94 ページ\)](#) (必須)
- [SIP 電話へのバックアップ レジストラ サービスの設定 \(96 ページ\)](#) (必須)
- [SIP 電話へのバックアップ レジストラ サービスの設定 \(オプション コマンドを使用\) \(99 ページ\)](#) (任意)
- [SIP レジストラ設定の確認 \(103 ページ\)](#) (任意)
- [プロキシ ダイアル ピア設定の確認 \(104 ページ\)](#) (任意)

SIP レジストラの設定

SIP レジストラとなるローカル SIP ゲートウェイはバックアップ SIP プロキシとして機能し、SIP 電話からの SIP 登録メッセージを受け入れます。これがローカル SIP IP Phone のロケーションデータベースになります。

レジストラは SIP 登録要求を受け入れ、動的に VoIP ダイアル ピアを構築するため、Cisco IOS 音声ゲートウェイ ソフトウェアが SIP 電話にコールをルーティングできるようになります。


SIP 登録要求に DNS アドレスを含む連絡先ヘッダーがあれば、その連絡先ヘッダーは、連絡先が SIP レジストラ データベースに追加される前に解決されます。これは、WAN 障害が発生している (および、その結果 Cisco Unified SIP SRST が機能している) 間に、DNS サーバが使用できなくなるためです。

SIP レジストラ機能は、次の設定によりイネーブルとなります。デフォルトでは、Cisco Unified SIP SRST はイネーブルではなく、SIP 登録メッセージを受け入れることができません。着信 SIP 登録メッセージを受け入れるには、次の設定をセットアップする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **allow-connections sip to sip**
5. **sip**
6. **registrar server [expires [max sec] [min sec]]**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
手順 1	<code>enable</code> 例: Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none">プロンプトが表示されたら、パスワードを入力します。
手順 2	<code>configure terminal</code> 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	<code>voice service voip</code> 例: Router(config)# voice service voip	音声サービス コンフィギュレーション モードを開始します。
手順 4	<code>allow-connections sip to sip</code> 例: Router(config-voi-srv)# allow-connections sip to sip	SIP から SIP エンドポイントへの接続を許可します。
手順 5	<code>sip</code> 例: Router(config-voi-srv)# sip	SIP コンフィギュレーション モードを開始します。
手順 6	<code>registrar server [expires [max sec] [min sec]]</code> 例: Router(conf-serv-sip)# registrar server expires max 600 min 60	SIP レジストラ機能をイネーブルにします。キーワードと引数が次のように定義されます。 <ul style="list-style-type: none">expires: (任意) 着信登録のアクティブ時間を設定します。max sec: (任意) 登録が期限切れになるまでの最大時間(秒単位)。指定できる範囲は 600 ~ 86400 です。デフォルトは 3600 です。  (注) 登録の期限切れタイムアウトは、TCP からの切断を防止するために、必ず TCP 接続エージングタイムアウトよりも小さい値に設定します。 <ul style="list-style-type: none">min sec: (任意) 登録が期限切れになるまでの最小時間(秒単位)。指定できる範囲は 60 ~ 3600 です。デフォルトは 60 です。
手順 7	<code>end</code> 例: Router(conf-serv-sip)# end	特権 EXEC モードに戻ります。

次の作業

着信 SIP 登録メッセージが正常に受信されるようにするには、音声レジスタ プールを設定する必要があります。「[SIP 電話へのバックアップ レジストラ サービスの設定](#)」セクション(96 ページ)

SIP 電話へのバックアップ レジストラ サービスの設定

SIP IP Phone へのバックアップ レジストラ サービスは、SIP ゲートウェイの音声レジスタ プールを設定することで提供できます。音声レジスタ プール設定では登録権限を制御することができ、さらに、SIP 電話登録がプールに一致する場合に、動的に作成された VoIP ダイアルピアに適用されるダイアルピア属性を設定することができます。次のコールタイプがサポートされています。

- SIP IP Phone の送受信：
 - ローカル PSTN
 - ローカルなアナログ FXS 電話機
 - ローカルな SIP IP Phone

次の設定のコマンドは、登録権限を制御して、基本的な音声レジスタ プールを設定します。プールは、Cisco Unified SIP SRST デバイスがどの登録を承認し、どれを拒否するかをユーザが制御できるようにします。このプールに一致する登録は、これらの設定に設定されたダイアルピア属性で VoIP SIP ダイアルピアを作成します。**id** コマンドのみ必須ですが、この設定例では、基本機能を示しています。

コマンドレベルの詳細については、『[Cisco Unified SRST and Cisco Unified SIP SRST Command Reference \(All Versions\)](#)』の適切なコマンド ページを参照してください。

前提条件

- SIP レジストラは、音声レジスタ プールのセットアップの前に設定する必要があります。詳細については、「[SIP レジストラの設定](#)」セクション(94 ページ)を参照してください。

制約事項

- **id** コマンドは、設定される個別の SIP IP Phone または SIP IP Phone のセットを特定します。したがって、ステップ 5 で設定した **id** コマンドが必要であり、他の音声レジスタ プールのコマンドの前に設定する必要があります。**mac address** キーワードおよび引数を使用する場合、電話機の MAC アドレスがルータの Address Resolution Protocol (ARP) キャッシュに表示されるように、IP Phone がルータの LAN インターフェイスと同じサブネット内にある必要があります。MAC アドレスが特定の音声レジスタ プール向けに設定されたら、新しい MAC アドレスに変更する前に既存の MAC アドレスを削除します。
- プロキシのダイアルピアは、PSTN から Cisco Unified SIP SRST へのすべてのコールをルーティングする自動生成ダイアルピアです。SIP 電話が Cisco Unified SIP SRST に登録され、**proxy** コマンドがイネーブルになると、2つのダイアルピアが自動的に作成されます。最初のダイアルピアはプロキシヘルレーティングされ、第2(またはフォールバック)のダイアルピアは SIP 電話にルーティングされます。静的なダイアルピアを正しく作成する(プロキシを指し示すダイアルピアを手動で作成する)方法でも、同じ機能を達成できます。プロキシのダイアルピアは1つのプロキシの IP アドレスのみをモニタできます。つまり、一度にモニタできるのは音声レジスタ プールからの1つのプロキシに限られます。複数のプロキシアドレスをモニタする必要がある場合は、手動で追加のダイアルピアを作成して設定します。



(注) SIP プロキシをモニタするには、ステップ 3 に記載されたとおり **call fallback active** コマンドを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **call fallback active**
4. **voice register pool tag**
5. **id {network address mask mask | ip address mask mask | mac address}**
6. **preference preference-order**
7. **proxy ip-address [preference value] [monitor probe {icmp-ping | rtr} [alternate-ip-address]]**
8. **voice-class codec tag**
9. **application application-name**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
手順 1	enable 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	configure terminal 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	call fallback active 例: Router(config)# call fallback active	(任意) ネットワーク 輻輳の場合、コール要求が代替ダイヤル ピアにフォールバックできるようにします。 • このコマンドは、プロキシのダイヤル ピアをモニタして、次の推奨ダイヤル ピアにフォールバックする場合に使用されます。 call fallback active コマンドの詳細については、『 PSTN Fallback Feature 』を参照してください。
手順 4	voice register pool tag 例: Router(config)# voice register pool 12	SIP 電話の音声レジスタ プール コンフィギュレーション モードを開始します。 • このコマンドは、どの登録が Cisco Unified SIP SRST デバイスによって承認または拒否されるかを制御するために使用します。

コマンドまたはアクション	目的
<p>手順 5 <code>id {network address mask mask ip address mask mask mac address}</code></p> <p>例: Router(config-register-pool)# id network 172.16.0.0 mask 255.255.0.0</p>	<p>ローカルに使用できる個別の SIP IP Phone またはそのセットを明示的に識別します。キーワードと引数が次のように定義されます。</p> <ul style="list-style-type: none"> • network address mask mask: network address mask mask のキーワードと引数の組み合わせは、指示された IP サブネット内の任意の IP Phone から指示された電話番号に対して SIP 登録メッセージを受け入れるために使用されます。 • ip address mask mask: ip address mask mask のキーワードと引数の組み合わせは、個別の電話機を識別するために使用されます。 • mac address: 特定の Cisco Unified IP Phone の MAC アドレスです。
<p>手順 6 <code>preference preference-order</code></p> <p>例: Router(config-register-pool)# preference 2</p>	<p>作成する VoIP ダイアル ピアのプリファレンス順序を設定します。範囲は 0 ~ 10 です。デフォルトは 0 です。これが最も高いプリファレンスです。</p> <ul style="list-style-type: none"> • このプリファレンスは、proxy コマンド内の preference キーワードで設定されたプリファレンスよりも大きい(優先順位が低い)必要があります。
<p>手順 7 <code>proxy ip-address [preference value] [monitor probe {icmp-ping rtr} [alternate-ip-address]]</code></p> <p>例: Router(config-register-pool)# proxy 10.2.161.187 preference 1</p>	<p>Cisco Unified SIP IP Phone が Cisco Unified SIP SRST ゲートウェイに登録を行うたびに、追加の VoIP ダイアル ピアが主要 SIP プロキシに到達します。キーワードと引数が次のように定義されます。</p> <ul style="list-style-type: none"> • ip-address: SIP プロキシの IP アドレス。 • preference value: (任意)作成されたプロキシのダイアル ピアのプリファレンスを定義します。このプリファレンスは、preference コマンドで設定されたプリファレンスよりも小さい(優先順位が高い)必要があります。 範囲は 0 ~ 10 です。プリファレンスの最大値は 0 です。デフォルトはありません。 • monitor probe: (任意)プロキシ ダイアル ピアのモニタリングをイネーブルにします。 • icmp-ping: ICMP ping を使用してプロキシ ダイアル ピアのモニタリングをイネーブルにします。 <p>(注) プローブが設定されたダイアル ピアは、発信コールでのみコールルーティングから除外されます。着信コールはこのダイアル ピアを介して届くことができます。</p> <ul style="list-style-type: none"> • rtr: RTR プロブを使用してプロキシ ダイアル ピアのモニタリングをイネーブルにします。 • alternate-ip-address: (任意)プロキシアドレス以外の代替 IP アドレスのモニタリングをイネーブルにします。たとえば、ゲートウェイのフロントエンドを SIP プロキシでモニタします。

	コマンドまたはアクション	目的
手順 8	<code>voice-class codec tag</code> 例: Router(config-register-pool)# voice-class codec 15	音声クラス コーデック パラメータを設定します。 <i>tag</i> 引数は、1 ~ 10000 の間のコーデック グループ数値です。
手順 9	<code>application application-name</code> 例: Router(config-register-pool)# application SIP.App	(任意) VoIP ダイヤル ピアのセッションレベルのアプリケーションを選択します。 <i>application-name</i> 引数を使用して、特定の自動音声応答 (IVR) アプリケーションを定義します。
手順 10	<code>end</code> 例: Router(config-register-pool)# end	特権 EXEC モードに戻ります。

次の作業

この他にも機能を追加する音声レジスタ プール コマンドがありますが、それらは必須ではありません。これらのコマンドについては、「[SIP 電話へのバックアップ レジストラ サービスの設定 \(オプション コマンドを使用\)](#)」セクション(99 ページ)を参照してください。

SIP 電話へのバックアップ レジストラ サービスの設定(オプション コマンドを使用)

前の設定は、基本的な音声レジスタ プールをセットアップするものです。この手順の設定は、オプションの属性を追加して機能を増やすためのものです。

前提条件

- 前提条件は「[SIP 電話へのバックアップ レジストラ サービスの設定](#)」セクション(96 ページ)に記載のとおりです。
- 「[SIP 電話へのバックアップ レジストラ サービスの設定](#)」セクション(96 ページ)の説明に従って、必要なコマンドを設定します。
- 「`alias`」コマンドを設定する前に、`translate-outgoing` (音声レジスタ プール) コマンドを使用してトランスレーションルールを設定する必要があります。

手順の概要

1. `enable`
2. `configure terminal`
3. `voice register pool tag`
4. `translation-profile outgoing profile-tag`
5. `alias tag pattern to target [preference value]`
6. `cor {incoming | outgoing} cor-list-name {cor-list-number starting-number [- ending-number] | default}`

7. **incoming called-number** [*number*]
8. **number tag number-pattern** {**preference value**} [**huntstop**]
9. **dtmf-relay** [**cisco-rtp**] [**rtp-nte**] [**sip-notify**]
10. **end**

手順の詳細

	コマンドまたはアクション	目的
手順 1	enable 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	configure terminal 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	voice register pool tag 例: Router(config)# voice register pool 12	音声レジスタ プール コンフィギュレーション モードを開始します。 • このコマンドは、どの登録が Cisco Unified SIP SRST デバイスによって承認または拒否されるかを制御するために使用します。
手順 4	translation-profile outgoing profile-tag 例: Router(config-register-pool)# voice translation-rule 1 rule 1 /1000/ /1006/ ! ! voice translation-profile 1 translate called 1 ! voice register pool xxx translation-profile outgoing 1	このコマンドは、トランスレーション プロファイルを特定の電話番号または SIP 電話のすべての電話番号に適用するために使用します。 • <i>Profile-tag</i> : 発信コールへの変換を処理するトランスレーション プロファイル名。

コマンドまたはアクション	目的
<p>手順 5 <code>alias tag pattern to target [preference value]</code></p> <p>例: Router(config-register-pool)# alias 1 94... to 91011 preference 8</p>	<p>主要なプロキシが使用できないと使用できない電話番号への着信 PSTN コールを、Cisco Unified SIP IP Phone が処理できるようにします。キーワードと引数が次のように定義されます。</p> <ul style="list-style-type: none"> • tag: 1 から 5 までの数字であり、複数の alias コマンドがある場合にそれらを区別する要素です。 • pattern: プレフィックス番号であり、着信電話番号と一致し、ワイルドカードを含めることができます。 • to: 代替番号にタグ番号パターンを接続します。 • target: ターゲット番号であり、番号パターンに一致する着信コールをルーティングする代替電話番号です。 • preference value: (任意) エリアスにダイヤルピアのプリファレンス値を割り当てます。value 引数は関連付けられたダイヤルピアの値で、範囲は 1 ~ 10 です。デフォルトはありません。
<p>手順 6 <code>cor {incoming outgoing} cor-list-name {cor-list-number starting-number [-ending-number] default}</code></p> <p>例: Router(config-register-pool)# cor incoming call91 1 91011</p>	<p>電話番号に関連付けられた VoIP ダイヤルピアに制限クラス (COR) を設定します。COR は、どの着信ダイヤルピアがどの発信ダイヤルピアを使用してコールを発信できるかを指定します。各ダイヤルピアは、着信および発信 COR リストでプロビジョニングできます。キーワードと引数が次のように定義されます。</p> <ul style="list-style-type: none"> • incoming: 着信ダイヤルピアが使用する COR リスト。 • outgoing: 発信ダイヤルピアが使用する COR リスト。 • cor-list-name: COR リストの名前。 • cor-list-number: COR リストの識別子。作成できる COR リストの最大数は 4 であり、着信または発信ダイヤルピアで構成されます。 • starting-number: 終了番号が含まれている場合の電話番号範囲の開始。スタンドアロン数も使用できます。 • (任意) 全範囲を設定するインジケータ。 • ending-number: (任意) 電話番号範囲の終了。 • default: ルータに既存のデフォルト COR リストを使用するよう指示します。
<p>手順 7 <code>incoming called-number [number]</code></p> <p>例: Router(config-register-pool)# incoming called-number 308</p>	<p>動的に作成されたダイヤルピアに着信コールパラメータを適用します。number 引数はオプションであり、電話番号のプレフィックスを表す数字のシーケンスを示します。</p>

	コマンドまたはアクション	目的
手順 8	<pre>number tag number-pattern {preference value} [huntstop]</pre> <p>例: Router(config-register-pool)# number 1 50.. preference 2</p>	<p>Cisco Unified SIP IP Phone からの登録メッセージを処理するためにレジストラが許可する E.164 電話番号を示します。キーワードと引数が次のように定義されます。</p> <ul style="list-style-type: none"> • tag: 1 から 10 までの数字であり、複数の number コマンドがある場合にそれらを区別する要素です。 • number-pattern: SIP IP Phone から登録メッセージを処理するためにレジストラから許可される電話番号(ワイルドカードとパターンを含む)。 • preference value: (任意) 番号リストで優先順位を定義します。 • huntstop: (任意) ダイヤル ピアが話中の場合にハンティングを停止します。
手順 9	<pre>dtmf-relay [cisco-rtp] [rtp-nte] [sip-notify]</pre> <p>例: Router(config-register-pool)# dtmf-relay rtp-nte</p>	<p>SIP ゲートウェイがテレフォニー インターフェイスと IP ネットワークとの間のデュアル トーン多重周波数 (DTMF) トーンをリレーする方式を指定します。キーワードは次のように定義されます。</p> <ul style="list-style-type: none"> • cisco-rtp: (任意) Real-Time Transport Protocol (RTP) とシスコ独自のペイロードタイプを使用して DTMF トーンを転送します。 • rtp-nte: (任意) Named Telephony Event (NTE) ペイロードタイプを持つ RTP を使用して DTMF トーンを転送します。 • sip-notify: (任意) SIP NOTIFY メッセージを使用して DTMF トーンを転送します。
手順 10	<pre>end</pre> <p>例: Router(config-register-pool)# end</p>	<p>特権 EXEC モードに戻ります。</p>

例

show running-config コマンドからの次の部分出力は、音声レジスタ プール 12 が、172.16.0.0/16 ネットワークの内線番号 50xx が設定されている SIP IP Phone からのすべての登録を受け入れるように設定されていることを示します。プール 12 に一致する登録で自動生成されたダイヤル ピアには、このプール内で設定された属性があります。

```
.
.
.
voice register pool 12
  id network 172.16.0.0 mask 255.255.0.0
  number 1 50.. preference 2
  application SIP.app
  preference 2
  incoming called-number
  cor incoming allowall default
  translate-outgoing called 1
  voice-class codec 1
.
.
.
```

SIP レジストラ設定の確認

SIP レジストラと音声レジスタ プールのトラブルシューティングを行うには、次の手順を実行します。

手順の概要

1. debug voice register errors
2. debug voice register events
3. show sip-ua status registrar

手順の詳細

	コマンドまたはアクション	目的
手順 1	<p>debug voice register errors</p> <p>例:</p> <pre>Router# debug voice register errors *Apr 22 11:52:54.523 PDT: VOICE_REG_POOL: Contact doesn't match any pools *Apr 22 11:52:54.539 PDT: VOICE_REG_POOL: Register request for (33015) from (10.2.152.39) *Apr 22 11:52:54.539 PDT: VOICE_REG_POOL: Contact doesn't match any pools. *Apr 22 11:52:54.559 PDT: VOICE_REG_POOL: Register request for (33017) from (10.2.152.39) *Apr 22 11:53:04.559 PDT: VOICE_REG_POOL: Maximum registration threshold for pool(3) hit</pre>	<p>このコマンドを使用して、登録中に発生したエラーをデバッグします。</p> <p>特定の登録要求用に設定された音声レジスタ プールがない場合、「連絡先がどのプールとも一致しません(Contact doesn't match any pools)」というメッセージが表示されます。</p>
手順 2	<p>debug voice register events</p> <p>例:</p> <pre>Router# debug voice register events Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: Contact matches pool 1 Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: key(91011) contact(192.168.0.2) add to contact table Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: key(91011) exists in contact table Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: contact(192.168.0.2) exists in contact table, ref updated Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: Created dial-peer entry of type 1 Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: Registration successful for 91011, registration id is 257</pre>	<p>登録アクティビティを表示するには、debug voice register events コマンドを使用するだけで十分です。登録アクティビティには、プールの照合、登録の作成およびダイヤル ピアの自動作成などがあります。詳細やエラー条件を確認するには、debug voice register errors コマンドを使用します。</p> <p>電話番号 91011 が正常に登録され、<i>type 1</i> と報告されます。これは、既存の VoIP ダイヤル ピアがあることを意味します。</p>

	コマンドまたはアクション	目的
手順 3	<pre>show sip-ua status registrar</pre> <p>例:</p> <pre>Router# show sip-ua status registrar Line destination expires(sec) contact ===== ===== 91021 192.168.0.3 227 192.168.0.3 91011 192.168.0.2 176 192.168.0.2 95021 10.2.161.50 419 10.2.161.50 95012 10.2.161.50 419 10.2.161.50 95011 10.2.161.50 420 10.2.161.50 95500 10.2.161.50 420 10.2.161.50 94011 10.2.161.40 128 10.2.161.40 94500 10.2.161.40 129 10.2.161.40</pre>	このコマンドは、連絡先アドレスに現在登録されているすべての SIP エンドポイントを表示するために使用します。

プロキシダイヤルピア設定の確認

プロキシダイヤルピアのトラブルシューティングを支援するため、**proxy** コマンドで **icmp-ping** キーワードを使用するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **voice register pool tag**
3. **proxy ip-address [preference value] [monitor probe {icmp-ping | rtr} [alternate-ip-address]]**
4. **end**
5. **show voice register dial-peers**
6. **show dial-peer voice**

手順の詳細

	コマンドまたはアクション	目的
手順 1	<pre>configure terminal</pre> <p>例:</p> <pre>Router# configure terminal</pre>	このコマンドを使用して、グローバル コンフィギュレーション モードを開始します。
手順 2	<pre>voice register pool tag</pre> <p>例:</p> <pre>Router(config)# voice register pool 1</pre>	このコマンドを使用して、音声レジスタ プール コンフィギュレーション モードを開始します。
手順 3	<pre>proxy ip-address [preference value] [monitor probe {icmp-ping rtr} [alternate-ip-address]]</pre> <p>例:</p> <pre>Router(config-register-pool)# proxy 10.2.161.187 preference 1 monitor probe icmp-ping</pre>	icmp-ping でモニタするように proxy コマンドを設定します。

	コマンドまたはアクション	目的
手順 4	<pre>end</pre> <p>例: Router(config-register-pool)# end</p>	特権 EXEC モードに戻ります。
手順 5	<pre>show voice register dial-peers</pre> <p>例: Router# show voice register dial-peers dial-peer voice 40035 voip preference 5 destination-pattern 91011 session target ipv4:192.168.0.2 session protocol sipv2 voice-class codec 1</p> <pre>dial-peer voice 40036 voip preference 1 destination-pattern 91011 session target ipv4:10.2.161.187 session protocol sipv2 voice-class codec 1 monitor probe icmp-ping 10.2.161.187</pre>	このコマンドは、ダイヤル ピア設定を確認し、 icmp-ping モニタリングが設定されていることを確認するために使用します。

コマンドまたはアクション	目的
<p>手順 6 show dial-peer voice</p> <p>例:</p> <pre>Router# show dial-peer voice VoiceOverIpPeer40036 peer type = voice, information type = voice, description = `', tag = 40036, destination-pattern = `91011', answer-address = `', preference=1, CLID Restriction = None CLID Network Number = ` ' CLID Second Number sent source carrier-id = `', target carrier-id = `', source trunk-group-label = `', target trunk-group-label = `', numbering Type = `unknown' group = 40036, Admin state is up, Operation state is up, incoming called-number = `', connections/maximum = 0/unlimited, ! Default output for incoming called-number command DTMF Relay = disabled, modem transport = system, huntstop = disabled, in bound application associated: 'DEFAULT' out bound application associated: ' ' dnis-map = permission :both incoming COR list:maximum capability ! Default output for cor command outgoing COR list:minimum requirement ! Default output for cor command Translation profile (Incoming): Translation profile (Outgoing): incoming call blocking: translation-profile = ` ' disconnect-cause = `no-service' advertise 0x40 capacity_update_timer 25 addrFamily 4 oldAddrFamily 4 type = voip, session-target = `ipv4:10.2.161.187', technology prefix: settle-call = disabled ip media DSCP = ef, ip signaling DSCP = af31, ip video rsvp-none DSCP = af41,ip video rsvp-pass DSCP = af41 ip video rsvp-fail DSCP = af41, UDP checksum = disabled, session-protocol = sipv2, session-transport = system, req-qos = best-effort, acc-qos = best-effort, req-qos video = best-effort, acc-qos video = best-effort, req-qos audio def bandwidth = 64, req-qos audio max bandwidth = 0, req-qos video def bandwidth = 384, req-qos video max bandwidth = 0,</pre>	<p>ダイヤルピア 40036 で show dial-peer voice コマンドを使用し、モニターブローブステータスを確認します。</p> <p> (注) また、cor コマンドと incoming called-number コマンドの出力が強調表示されます。</p>

コマンドまたはアクション	目的
<pre> RTP dynamic payload type values: NTE = 101 Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122 S=123, ClearChan=125, PCM switch over u-law=0,A-law=8 RTP comfort noise payload type = 19 fax rate = voice, payload size = 20 bytes fax protocol = system fax-relay ecm enable fax NSF = 0xAD0051 (default) codec = g729r8, payload size = 20 bytes, Media Setting = flow-through (global) Expect factor = 0, Icpif = 20, Playout Mode is set to adaptive, Initial 60 ms, Max 300 ms Playout-delay Minimum mode is set to default, value 40 ms Fax nominal 300 ms Max Redirects = 1, signaling-type = cas, VAD = enabled, Poor QOV Trap = disabled, Source Interface = NONE voice class sip url = system, voice class sip rellxx = system, monitor probe method: icmp-ping ip address: 10.2.161.187, Monitored destination reachable voice class perm tag = ` Time elapsed since last clearing of voice call statistics never Connect Time = 0, Charged Units = 0, Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0 Accepted Calls = 0, Refused Calls = 0, Last Disconnect Cause is "", Last Disconnect Text is "", Last Setup Time = 0. </pre>	

次の作業

次に、Cisco Unified SRST の着信および発信コールを設定します。詳細については、「[コール処理の設定](#)」セクション(109 ページ)を参照してください。

詳細については、「[Cisco Unified SRST 機能の概要](#)」セクション(1 ページ)の章の「[その他の関連資料](#)」セクション(28 ページ)を参照してください。

■ 次の作業



コール処理の設定

この章では、SCCP 電話のコールを発着信するために 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。

この章では、SIP 電話の標準 RFC 3261 機能のサポートについても説明します。機能にはコールブロッキングとコール転送が含まれます。



(注) SIP 電話のコール処理の設定は、バージョン 4.0 および 3.4 にのみ適用されます。

目次

- [バックツーバック ユーザ エージェント モードを使用する SIP SRST 機能を設定するための前提条件 \(109 ページ\)](#)
- [バックツーバック ユーザ エージェント モードを使用する SIP SRST 機能の設定における制約事項 \(110 ページ\)](#)
- [SCCP SRST コール処理の設定について \(110 ページ\)](#)
- [バックツーバック ユーザ エージェント モードを使用する SIP SRST 機能の設定について \(111 ページ\)](#)
- [Cisco Unified SCCP SRST の設定方法 \(113 ページ\)](#)
- [Cisco Unified SIP SRST の設定方法 \(149 ページ\)](#)
- [オプション機能の設定方法 \(158 ページ\)](#)
- [コール処理の設定例 \(160 ページ\)](#)
- [次の作業 \(161 ページ\)](#)

バックツーバック ユーザ エージェント モードを使用する SIP SRST 機能を設定するための前提条件

- 「[Cisco Unified SRST 機能の概要](#)」セクション (1 ページ) の「[Cisco Unified SIP SRST を設定するための前提条件](#)」セクション (9 ページ) に説明されている前提条件をすべて満たします。
- SIP レジストラを設定します。SIP レジストラによって、ユーザが登録の承認または拒否を制御できます。着信 SIP 登録メッセージの承認を設定するには、「[SIP を用いた Cisco Unified IP Phone の設定](#)」セクション (93 ページ) を参照してください。

バックツーバック ユーザ エージェント モードを使用する SIP SRST 機能の設定における制約事項

- ・ 「Cisco Unified SRST 機能の概要」セクション(1 ページ)の「Cisco Unified SIP SRST の設定に関する制約事項」セクション(10 ページ)に説明されている制約事項を参照してください。

SCCP SRST コール処理の設定について

Cisco Unified SRST は、Cisco Unified CM より小さいコール処理機能セットを提供しており、これらの機能の設定の大部分は既存の Cisco Unified CM または Cisco Unified IP Phone の設定の有効化です。

- ・ [WAN リンク障害用の H.323 VoIP コール プリザベーション拡張機能\(110 ページ\)](#)
- ・ [電話料金詐欺行為防止\(110 ページ\)](#)

WAN リンク障害用の H.323 VoIP コール プリザベーション拡張機能

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役立つのは、ゲートウェイと他のエンドポイント(通常は Cisco Unified IP Phone)は同じサイトにあるものの、コール エージェントがリモートサイトにあり、接続障害が起りやすいような場合です。

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。

電話料金詐欺行為防止

シスコ ルータ プラットフォームに音声対応 Cisco IOS ソフトウェア イメージをインストールする場合、プラットフォーム上で適切な機能をイネーブルにして、電話ハッカーによる侵入の可能性を防止する必要があります。防止するための機能を、音声コールを処理するシスコ ルータの Unified Communications アプリケーションすべてに展開します。このアプリケーションには、Cisco Unified Communications Manager Express (CME)、Cisco Survivable Remote Site Telephony (SRST)、Cisco Unified Border Element (UBE)、Cisco IOS ベース ルータ、スタンドアロン アナログ および デジタル PBX、公衆電話交換網 (PSTN) ゲートウェイ、および Cisco コンタクトセンター VoiceXML ゲートウェイなどがあります。電話料金詐欺行為防止の詳細については、『[Cisco Unified Communications Manager Express System Administration Guide](#)』の「[Toll Fraud Prevention](#)」を参照してください。

バックツーバック ユーザ エージェント モードを使用する SIP SRST 機能の設定について

Cisco Unified SRST システムは、ローカルおよび SIP WAN ネットワーク全体にわたり、標準ベースの RFC 3261 機能をサポートする SIP 電話をサポートできます。Cisco Unified SIP SRST を備えた SIP 電話は、SCCP 電話の場合と同様の機能を使用して、SIP ネットワーク経由でコールを発信できます。たとえば、発信者 ID、スピードダイヤル、リダイヤルなどの大半の SCCP 電話機能が、今では SIP ネットワーク上でもサポートされているため、ユーザは SCCP または SIP を選択することができます。

また、Cisco Unified SIP SRST は、コールの受け入れと転送のみを行うリダイレクトサーバを使用していた Cisco SIP SRST 3.0 より多くの機能を備えた個別のコール エージェントであるバックツーバック ユーザ エージェント (B2BUA) を使用します。B2BUA コール エージェントの主な利点はコール転送です。これは、電話に代わってコールを転送するからです。また、コールパスのコール仲介者としてプレゼンスを維持します。

Cisco SIP SRST 3.4 は次のコールの組み合わせをサポートします。

- SIP 電話から SIP 電話へ
- SIP 電話から PSTN/ルータ音声ポートへ
- SIP 電話から SCCP 電話へ

Cisco Unified SIP SRST および Cisco SIP Communications Manager Express の共通機能

voice register dn、**voice register global**、**voice register pool** の各コンフィギュレーションモード コマンドには、Cisco Unified SIP CME および Cisco Unified SIP SRST のどちらの動作モードでもアクセスできます。ただし、これらのモード内のすべてのコマンドが SIP SRST モードでの使用を対象としているわけではありません。表 7-1 は、どのコマンドが CME または SRST 動作モードに関連しているかを示すサマリー ガイドです。

詳細については、個々のコマンドのコマンド リファレンス ページを参照してください。



(注) 表 7-1 はすべてを網羅しているわけではなく、これら以外にもコマンドが存在する場合があります。

表 7-1 Cisco Unified SRST および Cisco Unified CME のバージョン 3.4 における新規または拡張されたコマンド (コンフィギュレーションモード別)

コマンド	ダイヤルピア	音声登録モード	設定可能: Cisco Unified (SIP) CME および Cisco Unified SIP SRST	適用可能: Cisco Unified (SIP) CME の み
after-hour exempt	X	dn	X	—
auto-answer	—	dn	—	X
call forward	X	dn	X	—
huntstop	X	dn	X	—
label	—	dn	—	X

表 7-1 Cisco Unified SRST および Cisco Unified CME のバージョン 3.4 における新規または拡張されたコマンド(コンフィギュレーションモード別)(続き)

コマンド	ダイヤルピア	音声登録モード	設定可能: Cisco Unified (SIP) CME および Cisco Unified SIP SRST	適用可能: Cisco Unified (SIP) CME の み
label	—	dn	—	X
number	X	dn	X	—
preference	X	dn	X	—
application	X	global	X	—
authenticate	—	global	—	X
create	—	global	—	X
date-format	—	global	—	X
dst	—	global	—	X
external ring	—	global	X	—
file	—	global	—	X
hold-alert	—	global	—	X
load	—	global	—	X
logo	—	global	—	X
max-dn	—	global	X	—
max-pool	—	global	X	—
max-redirect	—	global	—	X
mode	—	global	X	—
mwi	—	global	—	X
reset	—	global	—	X
tftp-path	—	global	—	X
timezone	—	global	—	X
upgrade	—	global	—	X
URL	—	global	—	X
Voicemail	—	global	—	X
after-hour exempt	X	pool	X	—
application	X	pool	X	—
call-forward	—	pool	X	—
call-waiting	—	pool	—	X
codec	X	pool	X	—
description	—	pool	—	X
dnd-control	—	pool	—	X
dtmf-relay	—	pool	X	—
id	—	pool	X	—

表 7-1 Cisco Unified SRST および Cisco Unified CME のバージョン3.4 における新規または拡張されたコマンド(コンフィギュレーションモード別)(続き)

コマンド	ダイヤルピア	音声登録モード	設定可能: Cisco Unified (SIP) CME および Cisco Unified SIP SRST	適用可能: Cisco Unified (SIP) CME の み
keep-conference	—	pool	—	X
max-pool	—	pool	X	—
number	X	pool	X	—
preference	X	pool	X	—
proxy	X	pool	X	—
reset	—	pool	—	X
speed-dial	—	pool	—	X
template	—	pool	—	X
translation-profile	X	pool	X	—
type	—	pool	—	X
username	—	pool	—	X
vad	X	pool	X	—
anonymous	—	template	—	X
caller-id	—	template	—	X
conference	—	template	—	X
dnd-control	—	template	—	X
forward	—	template	—	X
transfer	—	template	—	X

Cisco Unified SCCP SRST の設定方法

コール処理の設定には、次の一連のタスクが含まれます。

- [着信コールの設定\(114 ページ\)](#)
- [発信コールの設定\(132 ページ\)](#)
- [時刻、曜日、または日付に基づくコールブロッキングの設定\(153 ページ\)](#)

着信コールの設定

着信コールの設定には、次のタスクを含めることができます。

- コール転送と再ルーティング
 - 話中信号または無応答時のコール転送の設定(114 ページ) (任意)
 - コール再ルーティングの設定(115 ページ) (任意)
 - コールピックアップの設定(118 ページ) (任意)
 - 転送の桁収集方法の設定(122 ページ)
- 電話番号の変換とトランスレーション
 - グローバルプレフィックスの設定(123 ページ) (任意)
 - 桁トランスレーションルールの有効化(125 ページ) (任意)
 - トランスレーションプロファイルの有効化(126 ページ) (任意)
 - トランスレーションプロファイルの確認(129 ページ) (任意)
- ハントと呼び出しのタイムアウト動作
 - ダイアルピアチャンネルハントの設定(130 ページ) (任意)
 - 話中タイムアウトの設定(131 ページ) (任意)
 - 呼び出しタイムアウトのデフォルトの設定(131 ページ) (任意)

話中信号または無応答時のコール転送の設定

Cisco Unified CM のフォールバック中に話中信号を受け取ったか、または無応答の着信コールは、1つ以上の E.164 番号へ転送するように設定できます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 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。
手順 2	call-forward busy directory-number 例: Router(config-cm-fallback)# call-forward busy 50..	Cisco IP Phone が話中の場合の別の番号へのコール転送を設定します。 <ul style="list-style-type: none"> • <i>directory-number</i>: 完全修飾 E.164 番号を表す選択された電話番号。この番号には、電話の内線番号内で右揃えした桁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。

	コマンドまたはアクション	目的
手順 3	<pre>call-forward noan directory-number timeout seconds</pre> <p>例:</p> <pre>Router(config-cm-fallback)# call-forward noan 5005 timeout 10</pre>	<p>Cisco IP Phone から応答が受信されない場合の別の番号へのコール転送を設定します。</p> <ul style="list-style-type: none"> • directory-number: 完全修飾 E.164 番号またはローカルな内線番号を表す選択された電話番号。この番号には、電話の内線番号内で右揃えした桁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。 • timeout seconds: コールが別の電話に転送されるまでの待ち時間を秒単位で設定します。<i>seconds</i> の範囲は 3 ~ 60000 です。
手順 4	<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>

例

次の例では、着信コールが話中の内線番号に到達するか、IP 電話の内線番号が非在席だった場合に、コールを内線番号 5005 に転送します。着信コールは 15 秒間呼び出した後に内線 5005 に転送されます。

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

次の例では、内線番号が話中または非在席の場合に、コール転送の内線番号を変換します。**call-forward busy** コマンドには、引数 50.. があり、呼び出された内線番号の最後の 2 桁の前に 50 が付加されます。その結果の内線番号が、元の内線番号が話中または非在席の場合に、着信コールの転送先となる番号です。たとえば、話中の内線番号 6002 への着信コールは、内線番号 5002 に転送され、話中の内線番号 3442 への着信コールは内線番号 5042 に転送されます。着信コールは 15 秒間呼び出した後に転送されます。

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

コール再ルーティングの設定



(注)

default-destination コマンドは廃止されるため、**default-destination** コマンドの代わりに、**alias** コマンドを推奨します。

alias コマンドは、フォールバック中に使用できない電話番号へコールを再ルーティングするメカニズムを提供します。Cisco Unified Communications Manager のフォールバック中に使用できない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 ルールを作成できます。エイリアス ルールのセットは、**alias** コマンドを使用して作成されます。エイリアスは、設定した **alternate-number** エイリアスに一致する電話番号の電話が登録されたときに有効化されます。その状況で、着信コールが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るため、複数の異なる番号を同じ番号に再ルーティングできます。

設定された *alternate-number* は、特定の E.164 電話番号または Cisco Unified SRST ルータに登録済みの IP Phone に属する内線番号である必要があります。*alternate-number* に一致する番号の IP Phone が登録されると、追加の POTS ダイアル ピアが作成されます。接続先パターンは初期設定された *number-pattern* に設定され、POTS ダイアル ピア音声ポートは *alternate-number* に関連付けられた音声ポートに一致するように設定されます。

初期 *number-pattern* 範囲内の特定の電話番号を持つ他の IP Phone が登録された場合は、コールは *alternate-number* ではなく、その IP Phone にルーティングされます(通常のダイアルピア最長一致、プリファレンス、およびハントストップ ルールに従う)。

コール転送先

cfw キーワードで、話中または無応答のコールのコール転送先を設定できます。無応答時転送は、ユーザ設定可能な期間、電話を呼び出したが、コールが無応答で設定された接続先へ転送される場合として定義されています。話中転送および無応答時転送は、設定された文字列に設定でき、グローバルに設定されたコール転送設定をオーバーライドします。



(注)

グローバルに設定された設定は、*call-manager-fallback* モードの場合に選択され、SRST サービスに登録しているすべての電話に適用されます。

また、特定の番号に固有のコール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メリットは、SRST モードの間、そうでなければ到達不能な番号からのコールを使用可能な電話へ再ルーティングできる点です。1 番目の SRST 電話が話中の場合に、コールを 2 番目の SRST 電話に転送できるように、コール転送ルールを使用して基本ハント グループを確立できます。

また、**cfw** キーワードで、電話番号をそれ自体にエイリアスできるため、電話番号ごとの転送を設定できます。電話番号をそれ自体にエイリアスする例を以下に示します。内線番号 1001 の電話が登録されると、1001 に対して、コールをその電話にルーティングするダイアル ピアが自動的に作成されます。この初期ダイアル ピアの *call-manager-fallback* モードでのダイアルピア プリファレンス (**max-dn** コマンドで設定) が 2 に設定されると、ダイアル ピアは、自身のプリファレンス設定として 2 を使用します。

その後、**alias** コマンドを使用して、電話番号をそれ自体にエイリアスします。

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

この例では、1001 にコールをルーティングするが、プリファレンスが 1 で 2001 にコール転送する 1001 の 2 番目のダイアル ピアを作成しました。**alias** コマンドによって作成されたダイアルピアのプリファレンスが、ダイアル ピアが最初に作成したプリファレンスより小さい数値であるため、すべてのコールは最初に、**alias** コマンドによって作成されたダイアルピアに発信されます。そのように、グローバルに設定されている場合があるコール転送ではなく、**alias** コマンドによって設定されているとおりに転送されます。

個々のエイリアスのハントストップ

エイリアスの **huntstop** キーワードは、*call-manager-fallback* モードで **no huntstop** コマンドをグローバルに設定している場合のみ関係します。また、同じ *number-pattern* の複数の **alias** コマンドを使用し、エイリアス間での話中のハントを有効にする場合は、グローバルに **no huntstop** を設定する必要が生じることがあります。つまり、*number-pattern* の 1 つのエイリアスが試され、その後、電話が話中の場合は、*number-pattern* の 2 番目のエイリアスが試されます。

エイリアスの **huntstop** キーワードを指定すると、**no huntstop** コマンドによってハントストップがグローバルにオフである場合に、個々のエイリアスのハントストップ動作をオンに戻すことができます。個々のエイリアスに **huntstop** キーワードを設定するとそのエイリアスでハントが停止し、そのエイリアスがハント シーケンスの最終メンバーになります。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 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。
手順 2	alias tag number-pattern to alternate-number [preference preference-value] [cfw number timeout timeout-value] [huntstop] 例: Router(config-cm-fallback)# alias 1 60.. to 5001 preference 1 cfw 2000 timeout 10	Cisco Unified CM のフォールバック中に使用不能になる一連の電話へのコールの再ルーティングのルールセットを作成します。 <ul style="list-style-type: none"> • tag: エイリアス ルール範囲の ID。指定できる範囲は 1 ~ 50 です。 • number-pattern: 着信電話番号に一致するパターン。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。 • to: タグ番号パターンを代替番号へ接続します。 • alternate-number: 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 ルータでアクティブに登録されている IP Phone に属する特定の内線番号である必要があります。代替電話番号は複数の alias コマンドで使用できます。 • preference preference-value(任意): エイリアスにダイヤル ピアの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は 0 ~ 10 です。max-dn コマンドとともに使用します。 • cfw number(任意): cfw キーワードは、話中転送および無応答時転送を設定された文字列に設定し、グローバルに設定されたコール転送設定をオーバーライドできます。 • timeout timeout-value(任意): コール転送するための、呼び出し時の無応答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。 • huntstop(任意): 代替番号を試みた後にコール ハントを停止します。

	コマンドまたはアクション	目的
手順 3	<pre>max-dn max-directory-numbers [dual-line] [preference preference-order]</pre> <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ているすべての電話番号の VoIP ダイアル ピアを作成するため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"> • max-dn コマンドを使用して、alias コマンドで作成されるデフォルトのダイアル ピアのプリファレンスを設定します。 • コール再ルーティングを設定する場合は、max-dn preference を alias コマンドで設定されたプリファレンスより大きい数値のプリファレンスに設定します。
手順 4	<pre>end</pre> <p>例: Router(config-cm-fallback)# end</p>	<p>特権 EXEC モードに戻ります。</p>
手順 5	<pre>show dial-peer voice summary</pre> <p>例: Router# show dial-peer voice summary</p>	<p>音声ダイアル ピアの情報を表示します。</p> <ul style="list-style-type: none"> • ダイアル ピアに問題があると疑われる場合は、このコマンドを使用して、alias コマンドによって作成されたダイアル ピアを表示できます。

例

次の例では、**alias** コマンドの **preference** キーワードを **max-dn** コマンドによって作成されたプリファレンス値より小さい数値のプリファレンスに設定します。小さい値を設定することで、**cfw** キーワードを有効にすることができます。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にハントされ、1000 への無応答/話中コールは 2000 に転送されます。SRST モードでの他の内線番号への着信コールはすべて、10 秒後に 3000 に転送されます。

```
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 電話の PickUp ソフト キーが有効になります。その後、PickUp キーを押して、設定された *telephone-number* に一致する DID 着信者番号を持つ、現在呼び出し中の IP Phone に応答できます。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 電話を検索し、設定された *telephone-number* に一致する着信者番号を持つ呼び出し中のコールを見つけます。一致が見つかり、コールは、コールピックアップを要求した電話の内線番号へ自動的に転送されます。

SRST **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 に対応する Cisco Unified Communications Manager リリース 4.0(1) のデフォルトの電話ロードでは、フォールバック中に PickUp ソフト キーを有効にしません。Cisco 7905 および Cisco 7912 IP Phone の PickUp ソフト キーを有効にするには、デフォルトの電話ロードを Cisco Unified CM バージョン 4.0(1) Sr2 にアップグレードしてください。または、電話ロードをそれぞれ、`cmterm-7905g-sccp.3-3-8.exe` または `cmterm-7912g-sccp.3-3-8.exe` へアップグレードすることもできます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 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。
手順 2	<code>no huntstop</code> 例: Router(config-cm-fallback)# <code>no huntstop</code>	ハントストップを無効にします。
手順 3	<code>alias tag number-pattern to alternate-number</code> 例: Router(config-cm-fallback)# <code>alias 1 8005550100 to 5001</code>	Cisco Unified CM のフォールバック中に使用不能になる一連の電話へのコールの再ルーティングのルールセットを作成します。 <ul style="list-style-type: none"> • <code>tag</code>: エイリアス ルール範囲の ID。指定できる範囲は 1 ~ 50 です。 • <code>number-pattern</code>: 着信電話番号に一致するパターン。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。 • <code>to</code>: タグ番号パターンを代替番号へ接続します。 • <code>alternate-number</code>: 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 ルータでアクティブに登録されている IP Phone に属する特定の内線番号である必要があります。代替電話番号は複数の <code>alias</code> コマンドで使用できます。

	コマンドまたはアクション	目的
手順 4	<p><code>pickup telephone-number</code></p> <p>例: Router(config-cm-fallback)# pickup 8005550100</p>	すべての Cisco Unified IP Phone の PickUp ソフト キーを有効にし、SRST モードの間、いずれかの内線番号に発信された外部ダイヤルイン方式 (DID) コールに別の内線番号から応答できるようにします。 <i>telephone-number</i> 引数は、着信者番号に一致する電話番号です。
手順 5	<p><code>end</code></p> <p>例: Router(config-cm-fallback)# end</p>	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。次の **show running-config** コマンドからの部分出力は、**pickup** コマンドと **alias** コマンドが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提供するように設定されていることを示しています。

```
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 着信コールを受信した場合、**alias** コマンドは、コールを 4 つの内線番号 (5001 ~ 5004) のいずれかへ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、DID コールが内線番号 5002 を呼び出した場合、PickUp ソフト キーを押すことで、その他の内線番号 (5001、5003、5004) のいずれかからコールに応答することができます。

pickup コマンドは、着信 DID コールの着信者番号に基づいて一致を見つけることで動作します。この例では、着信者番号 (5001) が設定されたピックアップ番号 (800 555-0100) に一致しないため、内線番号 5004 から内線番号 5001 へのコール (内部コール) では **pickup** コマンドは有効化されません。つまり、**pickup** コマンドは、複数コールが同時に呼び出しを行っている場合に、内部コールと外部コールを区別します。

コンサルタティブ転送の設定

Cisco Unified SRST 4.3 より前のコンサルタティブ転送機能では、ダイヤル トーンが再生され、ダイヤルされた桁が収集されていました。桁は、コンサルタティブ転送、ブラインド転送、または PSTN 転送ブロッキングのパターンに一致するまで収集されました。コンサルタティブ転送の桁収集およびパターン マッチングの後に、時間外 (after-hours) ブロッキング基準が適用されました。

新機能では、転送の桁収集プロセスが変更され、Cisco Unified Communications Manager と一貫した方法になりました。この機能は、**call-manager-fallback** コンフィギュレーション モードで **transfer-system full-consult** コマンドが指定されており (デフォルト)、アイドル回線またはチャネルが捕捉、桁収集、およびダイヤルに使用可能な場合にのみサポートされます。

コンサルタティブ転送には 2 本の回線が必要です。転送元がオクトライン電話番号の場合、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。電話番号の最大数のチャネルが使用中である場合は、転送元の電話の別のアイドル回線が考慮されます。電話に **auto-line** コマンドが設定されている場合は、指定された自動回線 (アイドルの場合) が他の非自動回線より優先されます。アイドル回線が転送元の電話で使用できない場合は、コンサルタティブ転送ではなく、ブラインド転送が開始されます。

コンサルタティブ転送の間、転送元から転送先への回線は、同じ電話番号を共有する他の電話によって取得されるのを防ぐため、転送元の電話でロックされます。ユーザがコンサルタティブ転送のために Transfer ソフト キーを押すと、この捕捉されたコンサルタティブ転送コール レッグで桁がダイヤルされ収集されている間、Transfer ソフト キーは表示されません。コンサルタティブ転送パターン 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式は同じままですが、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ると、Cisco Unified SMST はコンサルタティブ転送コール レッグを終了し、Cisco IOS ソフトウェアにコールを転送するように通知し、その後、元のコールバブルを終了します。PARK FAC コードは、Cisco IOS ソフトウェアによって 10 秒タイマーを適用する必要がある新しいコールと同じ方法で処理されます。



(注)

デフォルトでは、拡張機能が新しいコール レッグから転送先番号の桁を収集します。必要に応じて、元のコール レッグから転送先番号の桁を収集するようにシステムを設定できます。「転送の桁収集方法の設定」セクション(122 ページ)を参照してください。

転送のブロッキングまたは桁間タイマーの期限切れによる転送の失敗のエラー処理はそのままです。これには、プロンプト行でのエラー メッセージの表示、「debug ephone error」が有効な場合のログへの記録、ファスト ビジーまたは話中音の再生、およびコンサルタティブ転送コール レッグの終了が含まれます。

これらの拡張機能をサポートするために、新しい設定は必要ありません。

会議コール

これらの会議コール拡張機能では、設定手順は必要ありません。

単一回線の電話番号

会議コールの開始側が単一回線電話番号で、電話に複数の電話番号が設定されている場合、システムは会議を作成するために、別の電話番号のアイドル チャネルを選択します。電話に複数の電話番号(デュアルラインまたは単一回線の電話番号)があり、それぞれがコールを保留している場合は、システムがユーザに会議コール用の回線を選択するように求めます。

デュアルラインの電話番号

会議コールの開始側がデュアルライン電話番号の場合、システムはデュアルライン電話番号から別のアイドル チャネルを選択します。選択したチャネルがコールを保留している場合は、会議操作によって自動的に保留チャネルが選択され会議が作成されます。

オクトラインの電話番号

会議コールの開始側がオクトライン電話番号の場合、システムは開始側の電話番号からアイドル チャネルを選択します。会議を完了するために、ユーザが新しいコールを確立する必要があります。同じ電話番号にアイドル チャネルがない場合は、同じ電話の他のアイドル電話番号またはチャネルは選択されません。同じ電話番号の他のチャネルまたは他の電話番号で既存のコールが保留中の場合、ユーザはそれら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 チャネルがない場合は、会議は中止され、「利用できる回線がありません(No Line Available)」というメッセージが示されます。

転送の桁収集方法の設定

デフォルトでは、転送先番号の桁は新しいコール レッグから収集されます。転送先番号の桁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 CM 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 モバイル アクセス ルータは、SRST をサポートしていません。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	enable 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	configure terminal 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	call-manager-fallback 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。

	コマンドまたはアクション	目的
手順 4	<pre>transfer-digit-collect {new-call orig-call}</pre> <p>例: Router(config-cm-fallback)# transfer-digit-collect orig-call</p>	<p>コンサルタティブ コールの転送に使用される桁収集方法を選択します。</p> <ul style="list-style-type: none"> • new-call: 桁は新しいコール レッグから収集されます。 • orig-call: 桁は元のコール レッグから収集されます。これは、Cisco Unified SRST 4.3 より前のバージョンでのデフォルトの動作でした。
手順 5	<pre>end</pre> <p>例: Router(config)# end</p>	<p>特権 EXEC モードに戻ります。</p>

例

次の例は、**transfer-digit-collect** 方法がレガシー値の **orig-call** に設定されていることを示しています。

```
!
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の桁を追加操作できます。このキーワードとその引数が使用される場合、内線番号パターンの先頭の桁が削除され、ダイヤルプランパターンの対応する先頭の桁で置換されます。このコマンドは、結果として 0101 などの 4 桁の内線番号になる 408 555-0101 などのダイヤルイン方式 (DID) 番号を避けるために使用できます。

グローバルプレフィックスは **dialplan-pattern** コマンドを使って設定します。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** キーワードはダイヤルの柔軟性を提供し、ダイヤルピアの E.164 番号がゲートキーパーに登録されるのを防ぎます。番号をその他のテレフォニーサービスで使用できるように、それらの番号をゲートキーパーに登録しないように選択できます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 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。
手順 2	dialplan-pattern tag pattern extension-length length [extension-pattern extension-pattern] [no-reg] 例: Router(config-cm-fallback)# dialplan-pattern 1 4085550100 extension-length 3 extension-pattern 4.. (注) この例では、内線番号 412 が 4085550112 に対応するように、すべての 4xx 内線番号を PSTN 番号 40855501xx にマッピングします。	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。 <ul style="list-style-type: none"> • tag: 10 桁の電話番号の前に使用されるダイヤルプラン文字列のタグ。タグ番号は 1 ~ 5 です。 • pattern: 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、および内線番号の残りの桁を示すワイルドカード マーカーである ドット(.)などのダイヤルプランパターン。 • extension-length: 内線番号の桁数を設定します。 • length: 内線番号の桁数。指定できる範囲は 1 ~ 32 です。 • extension-pattern: (任意) <i>pattern</i> 引数で定義される E.164 電話番号の先頭の桁とは異なる内線番号の先頭の桁パターンを設定します。 • extension-pattern: (任意) 内線番号の先頭の桁パターン。1 桁以上の数字とワイルドカード マーカーである ドット(.)で構成されます。たとえば、「5..」には内線番号 500 ~ 599 が含まれ、「5...」には内線番号 5000 ~ 5999 が含まれます。 • no-reg: (任意) ダイヤルピアの E.164 番号がゲートキーパーに登録されるのを防ぎます。
手順 3	exit 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、4085550 から始まる電話プレフィックスが付いた内線番号 101 ~ 199 のための dial-plan pattern 1 を作成する方法を示します。次の例が設定されると、ルータは 4085550144 が dial-plan pattern 1 に一致することを認識します。これは **extension-length** キーワードを使用して、最後の 3 桁の番号 144 を抽出し、着信コールの発信者 ID として提示します。

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

次の例では、内線番号の範囲が 400 ~ 499 になるように、3 桁の内線番号の先頭のプレフィックス桁を 0 から 4 に変換します。

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


次の例では、**dialplan-pattern** コマンドで、4085559 から始まる電話プレフィックスが付いた内線番号 801 ~ 899 のための **dial-plan pattern 2** を作成します。内線番号パターンの各数字が **number** コマンドで宣言され、2 つの POTS ダイアル ピアが作成されます。この例では、801 (内線番号) と 4085559001 (外線番号) です。

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

桁トランスレーションルールの有効化

桁トランスレーションルールは、Cisco Unified CM のフォールバック中に有効化できます。トランスレーションルールは、電話のエリアコードとプレフィックスコードを着信番号へ自動的に追加するなどの操作を実行する番号操作メカニズムです。



(注)

桁トランスレーションルールには多くの用途とバリエーションがあります。それらの詳細については、『[Cisco IOS Voice Configuration Library](#)』を参照してください。

Cisco SRST 3.2 以降および Cisco Unified SRST 4.0 以降を実行している場合は、次に説明するように **translate** コマンドを使用するのではなく、「[トランスレーションプロファイルの有効化](#)」セクション (126 ページ) に説明されている構成を使用してください。トランスレーションプロファイルは、Cisco SRST 3.2 で新たに導入され、追加機能を提供します。

トランスレーションルールは次のように使用できます。

- 音声コールの Answer Number Indication (ANI) (発信者番号) または着信番号識別サービス (DNIS) (着信者番号) の番号を操作するため。
- コールが着信ダイアル ピアに対応付けられる前、またはコールが発信ダイアル ピアによって転送される前に、電話番号を別の番号に変換するため。

システムに設定されたトランスレーションルールを表示するには、**show translation-rule** コマンドを使用します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 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。
手順 2	<code>translate {called calling}</code> <code>translation-rule-tag</code> 例: Router(config-cm-fallback)# translate called 20	Cisco Unified CM フォールバックがアクティブな間に、Cisco Unified IP Phone ユーザによってダイヤルまたは受信された電話番号を変更するためにトランスレーションルールを適用します。 <ul style="list-style-type: none"> • called: 発信コール番号にトランスレーションルールを適用します。 • calling: 着信コール番号にトランスレーションルールを適用します。 • translation-rule-tag: 1 ~ 2147483647 のトランスレーションルールの参照番号です。
手順 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、内線番号 1111 に着信するコールにトランスレーションルール 10 を適用します。Cisco Unified CM フォールバック中は、1111 への着信コールはすべて 2222 へ転送されます。

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

次は、桁トランスレーションルール 20 の設定例です。トランスレーションルールのプライオリティは 1(1 ~ 15 の範囲)で、完全な番号の省略表示(1234)が番号 2345 で置き換えられます。

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

トランスレーションプロファイルの有効化

Cisco SRST 3.2 以降および Cisco Unified SRST 4.0 以降は、トランスレーションプロファイルをサポートしています。トランスレーションプロファイルは、トランスレーションルールをグループ化し、トランスレーションルールを次に適用する方法の手順を示すために推奨される方法です。

- 着信者番号
- 発信者番号
- リダイレクトされた着信者番号

次の設定では、**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し、定義できます。ボイス トランスレーション プロファイル モードの **translate** コマンドは、着信者番号、発信者番号、またはリダイレクト先番号など、操作予定の番号のタイプを定義します。トランスレーション プロファイルを定義すると、その後、そのトランスレーション プロファイルを、ダイヤル ピアや音声ポートなどのさまざまな場所に適用できます。SRST の場合は、**call-manager fallback** モードでプロファイルを適用します。

Cisco IP Phone は、SRST モードの場合に、1 つの着信トランスレーション プロファイルと 1 つの発信トランスレーション プロファイルをサポートします。



(注)

Cisco SRST 3.2 以降のバージョンおよび Cisco Unified SRST 4.0 以降のバージョンの場合は、「[桁トランスレーション ルールの有効化](#)」セクション(125 ページ)で説明されているトランスレーション ルール設定の代わりに、以下に示す **voice translation-rule** コマンドと **translation-profile** コマンドを使用してください。ボイス トランスレーション ルールはトランスレーション ルールとは別の機能です。詳細については、『[Cisco IOS Voice Command Reference](#)』の **voice translation-rule** コマンドの説明を、トランスレーション ルールとプロファイルの一般的な情報については、『[VoIP Gateway Trunk and Carrier Based Routing Enhancements](#)』ドキュメントを参照してください。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
手順 1	voice translation-rule <i>number</i> 例: Router(config)# voice translation-rule 1	音声コールのトランスレーション ルールを定義し、 voice translation-rule コンフィギュレーション モードを開始します。 • <i>number</i> : トランスレーション ルールを識別する番号。範囲は 1 ~ 2147483647 です。
手順 2	rule <i>precedence/match-pattern/replace-pattern/</i> 例: Router(cfg-translation-rule)# rule 1/^9/ //	トランスレーション ルールを定義します。 • <i>precedence</i> : トランスレーション ルールのプライオリティ。範囲は 1 ~ 15 です。 • <i>match-pattern</i> : 着信コール情報を一致させるために使用される Stream Editor (SED) の表現。スラッシュ (/) はパターンデリミタです。 • <i>replace-pattern</i> : コール情報の一致パターンを置換するために使用される SED の表現。スラッシュ (/) はパターンデリミタです。

	コマンドまたはアクション	目的
手順 3	<p><code>exit</code></p> <p>例: Router(cfg-translation-rule)# exit</p>	voice translation-rule コンフィギュレーション モードを終了します。
手順 4	<p><code>voice translation-profile name</code></p> <p>例: Router(config)# voice translation-profile name1</p>	<p>音声コールのトランスレーション プロファイルを定義します。</p> <ul style="list-style-type: none"> name: トランスレーション プロファイルの名前。音声トランスレーション プロファイル名の最大長は 31 文字の英数字です。
手順 5	<p><code>translate {called calling redirect-called} translation-rule-number</code></p> <p>例: Router(cfg-translation-profile)# translate called 1</p>	<p>ボイス トランスレーション ルールをボイス トランスレーション プロファイルに関連付けます。</p> <ul style="list-style-type: none"> called: トランスレーション ルールを着信者番号に関連付けます。 calling: トランスレーション ルールを発信者番号に関連付けます。 redirect-called: トランスレーション ルールをリダイレクトされた着信者番号に関連付けます。 translation-rule-number: 1 ~ 2147483647 のトランスレーション ルールの参照番号です。
手順 6	<p><code>exit</code></p> <p>例: Router(cfg-translation-profile)# exit</p>	translation-profile コンフィギュレーション モードを終了します。
手順 7	<p><code>call-manager-fallback</code></p> <p>例: Router(config)# call-manager-fallback</p>	call-manager-fallback コンフィギュレーション モードを開始します。
手順 8	<p><code>translation-profile {incoming outgoing} name</code></p> <p>例: Router(config-cm-fallback)# translation-profile outgoing name1</p>	<p>Cisco IP Phone に着信コール レッグまたは発信コール レッグのトランスレーション プロファイルを割り当てます。</p> <ul style="list-style-type: none"> incoming: 着信コールにトランスレーション プロファイルを適用します。 outgoing: 発信コールにトランスレーション プロファイルを適用します。 name: トランスレーション プロファイルの名前。
手順 9	<p><code>exit</code></p> <p>例: Router(config-cm-fallback)# exit</p>	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、name1 という名前のトランスレーションプロファイルが2つのボイス トランスレーションルールで作成される設定を示します。rule1 は関連付けられた発信者番号で構成され、rule2 はリダイレクトされた着信者番号で構成されます。SRST モードの Cisco Unified IP Phone は name1 で設定されます。

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

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

トランスレーションプロファイルの確認

トランスレーションプロファイルを確認するには、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	<pre>show voice translation-rule number</pre> <p>例:</p> <pre>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</pre>	このコマンドを使用して、トランスレーションプロファイル用に定義したトランスレーションルールを確認できます。
手順 2	<pre>test voice translation-rule number input-test-string [type match-type [plan match-type]]</pre> <p>例:</p> <pre>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</pre>	このコマンドを使用して、トランスレーションプロファイルをテストできます。詳細については、『Cisco IOS Voice Command Reference』の test voice translation-rule コマンドの説明を参照してください。

ダイヤルピア チャネルハントの設定

ダイヤルピア ハント(ダイヤル ピアのグループを通じて使用可能な電話回線を検索)は、デフォルトでは、Cisco Unified CM フォールバック中は無効です。ダイヤルピア ハントを有効にするには、**no huntstop** コマンドを使用します。ダイヤルピア ハントの詳細については、『[Cisco IOS Voice Configuration Library](#)』を参照してください。

デュアルライン電話構成がある場合は、「[二重回線の電話設定](#)」セクション(85 ページ)を参照してください。**huntstop** コマンドで **channel** キーワードを使用すると、1 番目のチャンネルが話中か、応答がない場合に、着信コールは 2 番目のチャンネルをハントしなくなります。

チャンネルハントストップは、応答可能な人がいない回線の 1 番目のチャンネルでコールが 30 秒間呼出音を鳴らし、その後、さらに 30 秒間 2 番目のチャンネルで呼出音を鳴らしてから、別の回線にロールオーバーするような状況も防ぎます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 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。
手順 2	huntstop [channel] 例: Router(config-cm-fallback)# huntstop channel	Communications Manager のフォールバック中に作成された Cisco Unified IP Phone ダイヤル ピアに関連付けられたダイヤル ピアの huntstop 属性を設定します。 <ul style="list-style-type: none"> • デュアルライン構成の場合は、channel キーワードによって、1 番目のチャンネルが話中か、応答がない場合に、着信コールは 2 番目のチャンネルをハントしなくなります。
手順 3	exit 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、Cisco Unified CM のフォールバック中のダイヤルピア ハントと、デュアルライン電話構成での 2 番目のチャンネルへのハントを無効にしています。

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

話中タイムアウトの設定

このタスクは話中の接続先へのコール転送にタイムアウト値を設定します。話中タイムアウト値は、転送されたコールが話中信号を受け取ってから、コールが切断されるまでに経過可能な時間の長さです。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 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。
手順 2	timeouts busy seconds 例: Router(config-cm-fallback)# timeouts busy 20	コールが話中の接続先に転送された時点から切断されるまでの時間を設定します。 • <i>seconds</i> :秒数。範囲は 0 ~ 30 です。デフォルトは 10 です。 (注) このコマンドは話中の接続先へ転送されたコールに対してのみ話中タイムアウトを設定し、話中の接続先に直接ダイヤルしたコールのタイムアウトには影響しません。
手順 3	exit 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、話中の接続先へ転送されたコールのタイムアウトを 20 秒に設定しています。

```
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は、切断コードを発信者に返す前に、応答なしで電話の呼出音を鳴らすことができる時間の長さです。このタイムアウトによって、転送切断が監視されない Foreign Exchange Office (FXO) のようなインターフェイス上で着信したコールの切断を防止します。このタイムアウトは、無応答時コール転送が有効になっていない内線番号に対してのみ使用されます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 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。
手順 2	timeouts ringing seconds 例: Router(config-cm-fallback)# timeouts ringing 30	呼び出しタイムアウトのデフォルトを秒単位で設定します。指定できる範囲は 5 ~ 60000 です。デフォルト値はありません。
手順 3	exit 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、呼び出しタイムアウトのデフォルトを 30 秒に設定しています。

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

発信コールの設定

発信コールの設定には、次のタスクを含めることができます。

- コール転送の設定
 - ローカルおよびリモート コール転送の設定(133 ページ) (任意)
 - Cisco SRST 3.0 で H.450.2 および H.450.3 を使用したコンサルタティブ コールの転送および自動転送の有効化(133 ページ) (任意)
 - Cisco SRST 3.0 以前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(137 ページ) (任意)
- トランク アクセスコードの設定(141 ページ) (特定の条件下で必要)
- 桁間タイムアウト値の設定(142 ページ) (任意)
- 制限クラスの設定(143 ページ) (任意)
- 時刻、曜日、または日付に基づくコール ブロッキング(ツール バー)(147 ページ) (任意)

ローカルおよびリモート コール転送の設定

Cisco Unified IP Phone がローカル IP ネットワーク外部からの電話コールを別の Cisco Unified IP Phone へ転送できるように、Cisco Unified SRST を設定する必要があります。デフォルトでは、すべての Cisco Unified IP Phone の電話番号または仮想音声ポートが転送先として許容されます。最大 32 の転送パターンを入力できます。

コール転送設定は、**transfer-pattern** コマンドを使用して実行されます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 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。
手順 2	transfer-pattern transfer-pattern 例: Router(config-cm-fallback)# transfer-pattern 52540..	指定された転送パターンを使用して、非 IP 電話番号からのコールを同じ IP ネットワーク上の別 Cisco Unified IP Phone へ転送できるようにします。 <ul style="list-style-type: none"> • transfer-pattern: 許可されるコール転送の数字列。ワイルドカードを使用できます。
手順 3	exit 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** コマンドによって、非 IP 電話番号から、同じ IP ネットワーク上の番号が 5550100 ~ 5550199 の範囲内の任意の Cisco Unified IP Phone への転送を許可します。

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

Cisco SRST 3.0 で H.450.2 および H.450.3 を使用したコンサルタティブ コールの転送および自動転送の有効化

H.450.2 を使用したコンサルタティブ コールの転送により、ITU-T H.450.2 および H.450.3 標準を使用するコール レッグでコール転送とコール自動転送を開始するためのサポート機能が追加されます。H.450.2 と H.450.3 を使用したコール転送とコール自動転送は、ブラインド転送またはコンサルタティブ転送のいずれかとなります。ブラインド コール転送とブラインド コール自動転送は、呼出音を鳴らし始める前に、転送側の電話が発信者を宛先回線に接続する転送です。コンサルタティブ転送は、転送側が発信者を呼び出し中の電話(リングバックが鳴っている)に接続するか、または発信者を転送先に接続する前に転送側と転送先が通話する転送です。



(注)

Cisco SRST 3.1 以降および 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コール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

- 打診を行うコール転送は、2番目の回線またはコールインスタンスが IP Phone でサポートされている場合のみ使用できます。**max-dn** コマンドの **dual-line** キーワードを確認してください。
- VoIP ネットワーク内のすべての音声ゲートウェイ ルータが H.450 標準をサポートしている必要があります。
- VoIP ネットワーク内のすべての音声ゲートウェイ ルータが次のソフトウェアを実行している必要があります。
 - Cisco IOS リリース 12.3(2)T 以降のリリース
 - Cisco SRST 3.0


制約事項

ルータ間の H.450.12 補足サービス機能交換は実装されません。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
手順 1	<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>
手順 2	<pre>call-forward pattern pattern</pre> <p>例: Router(config-cm-fallback)# call-forward pattern 4...</p>	<p>コール自動転送用に H.450.3 標準を指定します。</p> <ul style="list-style-type: none"> • <i>pattern</i>: H.450.3 標準を使用するコール転送のために一致させる桁。着信した発信者番号がパターンと一致した場合は、H.450.3 標準を使用して自動転送できます。パターン .T は H.450.3 標準を使用してすべての発信者を自動転送します。
手順 3	<pre>transfer-system {blind full-blind full-consult local-consult}</pre> <p>例: 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 ポート上の場合にはサポートされません。</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"> • blind: 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。 <p> (注) blind キーワードは推奨されていません。代わりに、full-blind または full-consult キーワードのいずれかを使用してください。</p> <ul style="list-style-type: none"> • full-blind: 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。 • full-consult: 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 full-blind にフォールバックします。 • local-consult: 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。ローカル以外の打診またはローカル以外の転送先の場合、コールは blind にフォールバックします。
手順 4	<pre>transfer-pattern transfer-pattern</pre> <p>例: 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"> • <i>transfer-pattern</i>: 許可されるコール転送の数字列。ワイルドカードを使用できます。

	コマンドまたはアクション	目的
手順 5	<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。 ワンポイントアドバイス call-manager-fallback コンフィギュレーション モードを終了する前に、Cisco Unified SRST 電話ネットワーク全体を対象に設定する必要がある他のパラメータを設定します。
手順 6	<code>voice service voip</code> 例: <code>Router(config)# voice service voip</code>	(任意)音声サービス コンフィギュレーション モードを開始します。
手順 7	<code>h323</code> 例: <code>Router(conf-voi-serv)# h323</code>	(任意)H.323 音声サービス コンフィギュレーション モードを開始します。
手順 8	<code>h450 h450-2 timeout {T1 T2 T3 T4} milliseconds</code> 例: <code>Router(conf-serv-h323)# h450 h450-2 timeout T1 750</code>	(任意)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。このコマンドは基本的に、これらのタイマーのデフォルト設定がネットワーク遅延パラメータと一致しないときに使用されます。これら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。 <ul style="list-style-type: none"> • T1: 応答を特定するために待機するタイムアウト値。デフォルトは 2000 です。 • T2: コールセットアップを待機するタイムアウト値。デフォルトは 5000 です。 • T3: 応答を開始するために待機するタイムアウト値。デフォルトは 5000 です。 • T4: 応答のセットアップを待機するタイムアウト値。デフォルトは 5000 です。 • <i>milliseconds</i>: 時間(ミリ秒単位)。範囲は 500 ~ 60000 です。
手順 9	<code>end</code> 例: <code>Router(conf-serv-h323)# end</code>	(任意)特権 EXEC モードに戻ります。

例

次の例では、Cisco Unified SRST ルータによって処理されるすべての IP Phone を対象に、H.450.2 標準を使用して打診を行う転送を指定しています。

```
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

```

The following example enables call forwarding using the H.450.3 standard:

```

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 以前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 コール転送によって、アナログ電話でも、フックフラッシュを使用して転送を開始することで、打診を行ってコールを転送できます。フックフラッシュとは、電話が PBX からのダイヤルトーンの再呼び出しを試行していることを示すために、通常、コール中に電話同様のデバイスによって生成される短いオンフック期間を指しています。フックフラッシュは、多くの場合、コール転送を実行するために使用されます。たとえば、フックフラッシュは、アナログ電話のハンドセットの受け台にあるボタンを発信者がすばやく 1 回タップすると発生します。

この機能には、Tool Command Language (TCL) スクリプトのインストールが必要です。スクリプト `app-h450-transfer.tcl` を Cisco Software Center (<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp>) からダウンロードし、Cisco Unified SRST ルータが使用可能な TFTP サーバにコピーするか、Cisco Unified SRST ルータ上のフラッシュ メモリにコピーします。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、グローバル 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** コマンドの属性/値 (AV) ペアを使用して値を渡すことができるパラメータがあります。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てアナログ電話からのコール転送中に、コンサルタティブ コールのセットアップを早めたり、遅らせたりします。すべての桁が収集された時点で、遅延タイマーが始動します。受信側へのコールセットアップは遅延タイマーが切れるまで開始されません。遅延タイマーが期限切れになる前に転送側がオンフックになると、転送はコンサルタティブ転送ではなくブラインド転送と見なされます。接続先の電話の呼び出し中または接続先側による応答後のいずれかに、遅延タイマーが切れ転送側がオンフックになると、転送はコンサルタティブ転送と見なされます。

TCL スクリプトに加えて、`ReadMe` ファイルにもスクリプトと設定可能な AV ペアが説明されています。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、追加のスクリプト固有の情報が含まれる場合があるため、新しいバージョンのスクリプトをダウンロードするたびにこのファイルを参照してください。



(注)

Cisco SRST 3.1 以降のバージョンおよび 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

- app-h450-transfer.tcl という名前の H.450 TCL スクリプトを Cisco Software Center からダウンロードする必要があります。次のバージョンのスクリプトが入手可能です。
 - app-h450-transfer.2.0.0.2.tcl (Cisco IOS リリース 12.2(11)YT1 以降のリリース用)
 - app-h450-transfer.2.0.0.1.tcl (Cisco IOS リリース 12.2(11)YT 用)
- VoIP ネットワーク内のすべての音声ゲートウェイ ルータが 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 リリース 12.2(11)YT 以降のリリース
 - Cisco SRST V3.0 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)

Cisco IOS リリース 12.2(11)YT1 以降をインストールしている場合は、継続して app-h450-transfer.2.0.0.1.tcl スクリプトを使用できますが、Cisco IOS リリース 12.2(11)YT1 より前のリリースの Cisco IOS ソフトウェアでは app-h450-transfer.2.0.0.2.tcl スクリプトは使用できません。

制約事項

- フックフラッシュを使用したアナログ FXS 電話によってコンサルタティブ転送が行われた場合、最初の転送操作が完了し、転送元と転送先が接続されるまで、コンサルタティブ コールそのものをさらに転送することはできません (つまり、再帰転送またはチェーン転送にすることはできません)。最初のコール転送操作が完了し、転送元と転送先のみがコールの参加者である場合は、転送先側がさらにコールを転送できます。
- 打診を行うコール転送は、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の転送試行はブラインド転送として実行されます。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
手順 1	<pre>call application voice application-name location</pre> <p>例: 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"> application-name: IVR アプリケーションのユーザ定義の名前。この名前は、スクリプトのファイル名と一致している必要はありません。 location: URL 形式のスクリプトのディレクトリとファイル名。たとえば、フラッシュ メモリ (<code>flash:filename</code>)、TFTP (<code>tftp://.filename</code>) または HTTP サーバ (<code>http://.filename</code>) は有効な場所です。
手順 2	<pre>call application voice application-name language number language</pre> <p>例: Router(config)# call application voice transfer_app language 1 en</p>	<p>(任意) アプリケーションによって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"> application-name: ステップ 1 で割り当てられた IVR アプリケーションの名前。 number: IVR アプリケーションのオーディオ ファイルによって使用される言語を識別する番号。 language: プロンプトの言語を指定する 2 文字コード。有効な入力は、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。
手順 3	<pre>call application voice application-name set-location language category location</pre> <p>例: Router(config)# call application voice transfer_app set-location en 0 flash:/prompts</p>	<p>アプリケーションによってダイナミック プロンプトに使用されるオーディオ ファイルの場所とカテゴリを定義します。</p> <ul style="list-style-type: none"> application-name: TCL IVR アプリケーションの名前。 language: プロンプトの言語を指定する 2 文字コード。有効な入力は、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。 category: この場所からのオーディオ ファイルのカテゴリ グループ (0 ~ 4)。値 0 は、すべてのカテゴリを意味します。 location: アプリケーションによって使用される言語オーディオ ファイルが格納されているディレクトリの URL。ファイル名は含めません。フラッシュ メモリ (<code>flash</code>) またはサーバ上のディレクトリ (<code>TFTP</code>、<code>HTTP</code>、または <code>RTSP</code>) はすべて有効です。 <p>プロンプトはアナログ FXS 電話からのコール転送の場合に必要です。IP Phone からのコール転送の場合は、プロンプトは不要です。</p>

コマンドまたはアクション	目的
<p>手順 4 <code>call application voice application-name delay-time seconds</code></p> <p>例: Router(config)# call application voice transfer_app delay-time 1</p>	<p>(任意)H.450 アプリケーションを使用してコール転送を実行するアナログ電話の場合に、コンサルタティブコールセットアップの遅延時間を設定します。このコマンドは、属性/値(AV)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"> <i>seconds</i>: コールセットアップを遅らせる秒数。範囲は 1 ~ 10 です。デフォルトは 2 です。 <p>一般に 2 秒を超える遅延はユーザに気付かれます。</p> <p>H.450 コール転送およびコール自動転送の AV ペアと TCL スクリプトの詳細については、スクリプトに付属の ReadMe ファイルを参照してください。</p>
<p>手順 5 <code>dial-peer voice number pots</code></p> <p>例: Router(config)# dial-peer voice 25 pots</p>	<p>POTS ダイアルピアを設定するためにダイアルピア コンフィギュレーションモードを開始します。</p>
<p>手順 6 <code>application application-name</code></p> <p>例: Router(config-dial-peer)# application transfer_app</p>	<p>ステップ 1 で名前が付けられたアプリケーションをダイアルピアにロードします。</p>
<p>手順 7 <code>exit</code></p> <p>例: Router(config-dial-peer)# exit</p>	<p>ダイアルピア コンフィギュレーションモードを終了します。</p> <p>ワンポイントアドバイス ダイアルピア コンフィギュレーションモードを終了する前に、このダイアルピアに設定する必要のあるその他のダイアルピアパラメータを設定します。</p>
<p>手順 8 <code>dial-peer voice number voip</code></p> <p>例: Router(config)# dial-peer voice 29 voip</p>	<p>VoIP ダイアルピアを設定するためにダイアルピア コンフィギュレーションモードを開始します。</p>
<p>手順 9 <code>application application-name</code></p> <p>例: Router(config-dial-peer)# application transfer_app</p>	<p>ステップ 1 で名前が付けられたアプリケーションをダイアルピアにロードします。</p>
<p>手順 10 <code>exit</code></p> <p>例: Router(config-dial-peer)# exit</p>	<p>ダイアルピア コンフィギュレーションモードを終了します。</p> <p>ワンポイントアドバイス ダイアルピア コンフィギュレーションモードを終了する前に、このダイアルピアに設定する必要のあるその他のダイアルピアパラメータを設定します。</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 秒に設定しています。

```
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)

通常のネットワークダイヤルプラン構成で、フォールバック中に使用するトランクアクセスを提供するために、相手先固定の POTS 音声ダイヤルピアが設定されないようにする場合にのみ、トランクアクセスコードを設定します。すでにローカル PSTN ポートに、ダイヤルピアによって提供された適切なアクセスコードが設定されている場合は(たとえば、9 をダイヤルすると FXO PSTN 回線が選択される)、この設定は不要です。

トランクアクセスコードは、Cisco Unified CM フォールバック中のみアクティブになる POTS 音声ダイヤルピアを作成することで、IP Phone に Cisco Unified CM フォールバック中の PSTN へのアクセスを提供します。音声ポート (BRI、E&M、FXO、および PRI) に適合できるこれらの一時ダイヤルピアによって、Cisco Unified IP Phone は Cisco Unified CM モードの間、トランク回線にアクセスできます。Cisco Unified SRST がアクティブな場合、同じタイプのすべての PSTN インターフェイスが同等に処理され、発信 PSTN コールを発信するためにいずれのポートも選択できます。

トランクアクセスコードは、**access-code** コマンドを使用して作成されます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 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。
手順 2	<code>access-code</code> {{ <code>fxo</code> <code>e&m</code> } <code>dial-string</code> { <code>bri</code> <code>pri</code> } <code>dial-string</code> [<code>direct-inward-dial</code>]} 例: Router(config-cm-fallback)# access-code e&m 8	Cisco Unified SRST が有効な場合に、Cisco Unified IP Phone が Cisco Unified Communications Manager のフォールバック モードでのみトランク回線にアクセスできるように、回線の各タイプのトランク アクセスコードを設定します。 <ul style="list-style-type: none"> • fxo: Foreign Exchange Office (FXO) インターフェイスを有効にします。 • e&m: アナログ Ear and Mouth (E&M) インターフェイスを有効にします。 • dial-string: ダイヤル ピアを作成することで指定された各回線タイプのダイヤル アクセスコードを設定する文字列。dial-string 引数は、指定された各回線タイプの一時ダイヤル ピアを設定するために使用されます。 • bri: BRI インターフェイスを有効にします。 • pri: PRI インターフェイスを有効にします。 • direct-inward-dial: (任意) POTS ダイヤル ピアのダイヤルイン方式 (DID) を有効にします。
手順 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、BRI のアクセスコード番号 8 を作成し、POTS ダイヤル ピアの DID を有効にしています。

```
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を設定するには、Cisco Unified SRST ルータに接続されているすべての Cisco Unified IP Phone が、最初の桁または後続の 1 桁がダイヤルされてから待機する長さを秒単位で指定します。**timeouts interdigit** タイマーは、発信者が桁を入力すると有効になり、宛先アドレスが特定されるまで、発信者が後続の桁を入力するたびに再起動されます。宛先アドレスが特定される前に設定されたタイムアウト値を超えると、トーンが鳴り、コールは終了されます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 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。
手順 2	timeouts interdigit seconds 例: Router(config-cm-fallback)# timeouts interdigit 5	(任意) 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。 • <i>seconds</i> : すべての Cisco Unified IP Phone の桁間タイムアウト期間(秒単位)。有効な入力値は 2 ~ 120 の整数です。
手順 3	exit 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、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、着信番号が不完全な状態で 5 秒が経過するとタイムアウトします。たとえば、必須の 10 桁 (4085550100) の代わりに 9 桁 (408555010) をダイヤルした発信者には、その秒数のタイムアウトが経過した後で話中音が聞こえます。

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

制限クラスの設定

制限クラス (COR) 機能は、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、特定のコール試行を拒否する機能です。この機能は、ネットワーク設計に柔軟性を提供し、それによってユーザはコールをブロックしたり (たとえば、900 番へのコール)、異なる発信者からのコール試行に異なる制限を適用したりすることができます。**cor** コマンドは、Cisco Unified CM のフォールバック中に作成された電話番号に関連付けられたダイヤル ピアのダイヤルピア COR パラメータを設定します。

着信コールおよび発信コールごとに最大 20 の COR リストを保持できます。デフォルトの COR は COR リスト番号または番号範囲が一致しない電話番号に割り当てます。割り当てられた COR はダイヤル ピア用に呼び出され、Communications Manager のフォールバック登録時に電話番号ごとに自動的に作成されます。

COR が着信ダイヤル ピア (着信コール) に適用され、それが発信ダイヤル ピア (発信コール) に適用された COR に等しいか、そのスーパーセットの場合は、コールは通過します。音声ポートは、コールが着信または発信のどちらと見なされるかを判別します。電話を Cisco Unified SRST ルータの FXS ポートに接続し、その電話から発信を試みると、コールはルータと音声ポートへの着信コールと見なされます。FXS 電話に発信した場合、コールは発信と見なされます。

デフォルトでは、着信コール レッグが最高の COR プライオリティとなり、発信コール レッグが最低のプライオリティとなります。ダイヤル ピアの着信コールに対する COR 設定がない場合は、ダイヤル ピアに接続された電話から発信できるため、コールはダイヤル ピアの COR 設定に関係なく、ダイヤル ピアから発信されます。表 7-2 は、COR リストの設定方法に基づいて、コールの機能について説明しています。

表 7-2 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	コールは成功します。
COR なし	COR リストは発信コールに適用される	コールは成功します。COR が適用されない場合、デフォルトでは、着信ダイヤル ピアが最高の COR プライオリティとなります。ダイヤル ピアに着信コール レッグの COR が適用されていない場合、ダイヤル ピアは、発信ダイヤル ピアの COR 設定に関係なく、他のダイヤル ピアから発信できます。
COR リストは着信コールに適用される	COR なし	コールは成功します。デフォルトでは、発信ダイヤル ピアは最低のプライオリティとなります。着信または発信ダイヤル ピアの着信コールに対していくつかの COR 設定があるため、それは、発信または終端側ダイヤル ピアの発信コールの COR 設定のスーパーセットです。
COR リストは着信コールに適用される (COR リストのスーパーセットが発信ダイヤル ピアの発信コールに適用される)	COR リストは発信コールに適用される (COR リストのサブセットが着信ダイヤル ピアの着信コールに適用される)	コールは成功します。着信ダイヤル ピアの着信コールの COR リストは、発信ダイヤル ピアの発信コールに対する COR リストのスーパーセットです。
COR リストは着信コールに適用される (COR リストのサブセットが発信ダイヤル ピアの発信コールに適用される)	COR リストは発信コールに適用される (COR リストのスーパーセットが着信ダイヤル ピアの着信コールに適用される)	コールは成功しません。着信ダイヤル ピアの着信コールの COR リストは、発信ダイヤル ピアの発信コールに対する COR リストのスーパーセットではありません。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 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。
手順 2	cor {incoming outgoing} cor-list-name [cor-list-number starting-number - ending-number default] 例: Router(config-cm-fallback)# cor outgoing LockforPhoneC 1 5010 - 5020	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"> • incoming: 着信ダイヤル ピアによって使用される COR リスト。 • outgoing: 発信ダイヤル ピアが使用する COR リスト。 • cor-list-name: COR リストの名前。 • cor-list-number: COR リスト ID。作成可能な最大 COR リスト数は 20 で、着信ダイヤル ピア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 設定がない電話番号は、デフォルトの COR リストに割り当てられます。 • starting-number - ending-number: 電話番号の範囲、たとえば、2000 ~ 2025。 • default: ルータに既存のデフォルト COR リストを使用するように指示します。
手順 3	exit 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、フォールバック中に作成された Cisco Unified IP Phone ダイヤル ピアと電話番号に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
```

次の例では、デフォルトの COR リスト内の Cisco IP Phone ダイヤル ピアと電話番号に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
```

次の例では、COR のサブセットまたはスーパーセットを作成する方法を示しています。まず、カスタム ダイヤルピア COR が、その下で宣言される名前で作成されます。

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

次の設定例では、COR リストが作成され、ダイヤル ピアに適用されます。

```
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、接続先番号 734...、1800.....、1900.....、316...、および 911 に 5 つのダイヤル ピアが設定されています。COR リストはダイヤル ピアごとに適用されます。

```
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
```

これで、COR リストが個別の電話番号に適用されます。

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

設定例では、次のことが可能です。

- 内線番号 1001 から番号 734...、911、316... へのコール
- 内線番号 1002 から番号 734...、1800、911、316... へのコール
- 内線番号 1003 ~ 1008 から候補となるすべての Cisco Unified SRST ルータの番号へのコール
- すべての内線番号から 316... へのコール

時刻、曜日、または日付に基づくコールブロッキング(トールバー)

電話の不正使用を防止するためのコールブロッキングは、指定の時刻、曜日、または日付に、指定の桁のパターンを一致させることで実装されます。最大 32 の桁のパターンを指定できます。コールブロッキングは IP Phone でのみサポートされ、アナログ Foreign Exchange Station (FXS) 電話ではサポートされていません。

コールブロッキングに定義された期間に、コールブロッキングに指定されたパターンと一致する桁にユーザが発信を試みると、ファスト ビジー信号が約 10 秒間再生されます。その後、コールは終了し、回線はオンフックステータスに戻ります。

SRST (call-manager-fallback コンフィギュレーション) モードでは、時間外のコールブロッキングに対する電話または PIN ベースの免除はありません。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 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。
手順 2	after-hours block pattern tag pattern [7-24] 例: Router(config-cm-fallback)# after-hours block pattern 1 91900	ブロックする発信桁のパターンを定義します。個別にコマンドを使用して、最大 32 のパターンを定義できます。 <ul style="list-style-type: none"> • 7-24 キーワードが指定された場合、パターンは、週 7 日、1 日 24 時間、常時ブロックされます。 • 7-24 キーワードが指定されていない場合は、パターンは after-hours day および after-hours date コマンドを使用して定義された日数および日付の間ブロックされます。

	コマンドまたはアクション	目的
手順 3	<pre>after-hours day day start-time stop-time</pre> <p>例: Router(config-cm-fallback)# after-hours day mon 19:00 7:00</p>	<p>after-hours block pattern コマンドを使用して定義された発信ダイヤルパターンへのコールがブロックされる曜日に基づいて、繰り返される期間を定義します。</p> <ul style="list-style-type: none"> <i>day</i>: 曜日の省略形。有効な曜日の省略形は、sun、mon、tue、wed、thu、fri、sat です。 <i>start-time stop-time</i>: コールブロッキングの開始時刻と終了時刻。HH:MM 形式の 24 時間制で指定します。停止時刻が開始時刻よりも早い時刻になっている場合、停止時刻は開始時刻の翌日になります。たとえば、「mon 19:00 07:00」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。
手順 4	<pre>after-hours date month date start-time stop-time</pre> <p>例: Router(config-cm-fallback)# after-hours date jan 1 0:00 0:00</p>	<p>after-hours block pattern コマンドを使用して定義された発信ダイヤルパターンへのコールがブロックされる月と日付に基づいて、繰り返される期間を定義します。</p> <ul style="list-style-type: none"> <i>month</i>: 月の省略形。有効な月の省略形は、jan、feb、mar、apr、may、jun、jul、aug、sep、oct、nov、dec です。 <i>date</i>: その月の日付。範囲は 1 ~ 31 です。 <i>start-time stop-time</i>: コールブロッキングの開始時刻と終了時刻。HH:MM 形式の 24 時間制で指定します。停止時刻は開始時刻よりも遅くする必要があります。値 24:00 は無効です。停止時刻に 00:00 を入力すると、23:59 に変更されます。開始時刻と停止時刻の両方に 00:00 を入力した場合、指定した日付の 24 時間全体でコールがブロックされます。
手順 5	<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

次の例では、発信コールがブロックされる番号パターンをいくつか定義します。パターン 1 および 2 は、「1」および「011」で始まる外部番号へのコールをブロックします。このブロックは、月曜日から金曜日の午前 7 時以前と午後 7 時以後、土曜の午前 7 時以前と午後 1 時以後、日曜(終日)に行われます。パターン 3 は、900 番へのコールを週 7 日、1 日 24 時間にわたってブロックします。

```
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
```


Cisco Unified SIP SRST の設定方法

ここでは、次の手順について説明します。

- [SIP 電話の機能の設定 \(149 ページ\)](#) (任意)
- [SIP 間のコール転送の設定 \(151 ページ\)](#) (必須)
- [時刻、曜日、または日付に基づくコールブロッキングの設定 \(153 ページ\)](#) (必須)
- [SIP のコール保留と保留解除 \(156 ページ\)](#) (設定は必要ありません)
- [例 \(156 ページ\)](#)

SIP 電話の機能の設定

音声レジスタ プールを設定した後、この手順は機能性を高めるためにオプション機能を追加します。機能によっては、プールごとに設定される場合もあれば、グローバルに設定される場合もあります。

voice register pool 設定では、現在、プールごとに複数の新しいオプションを設定できます (プールは 1 台の電話または電話のグループ)。また、Cisco Unified SIP SRST の新しい **voice register global** コンフィギュレーション モードもあります。**voice register global** モードでは、電話に特性をグローバルに割り当てることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice register global tag**
4. **max-pool max-voice-register-pools**
5. **application application-name**
6. **external ring {bellcore-dr1 | bellcore-dr2 | bellcore-dr3 | bellcore-dr4 | bellcore-dr5}**
7. **exit**
8. **voice register pool tag**
9. **no vad**
10. **codec codec-type [bytes]**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
手順 1	<code>enable</code> 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	<code>configure terminal</code> 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	<code>voice register global tag</code> 例: Router(config)# voice register global 12	音声レジスタ グローバル コンフィギュレーション モードを開始して、Cisco Unified SIP SRST 環境内でサポートされるすべての Cisco SIP IP Phone に対してグローバル パラメータを設定します。
手順 4	<code>max-pool max-voice-register-pools</code> 例: Router(config-register-global)# max-pool 10	Cisco Unified SIP SRST 環境内でサポートされる SIP 音声レジスタ プールの最大数を設定します。 <i>max-voice-register-pools</i> 引数は、Cisco Unified SIP SRST ルータによってサポートされる SIP 音声レジスタ プールの最大数を表します。音声レジスタ プールの上限は、バージョンとプラットフォームによって異なります。 Cisco IOS コマンドライン インターフェイス (CLI) のヘルプを参照してください。デフォルトは 0 です。
手順 5	<code>application application-name</code> 例: Router(config-register-global)# application global_app	SIP 電話に関連付けられたすべてのダイヤル ピアに対応するセッションレベルのアプリケーションを選択します。 <i>application-name</i> 引数を使用して、特定の自動音声応答 (IVR) アプリケーションを定義します。
手順 6	<code>external-ring {bellcore-dr1 bellcore-dr2 bellcore-dr3 bellcore-dr4 bellcore-dr5}</code> 例: Router(config-register-global)# external-ring bellcore-dr1	Cisco SIP または Cisco SCCP IP Phone で外部コールに使用される呼出音のタイプを指定します。標準 GR-506-CORE「LSSGR: Signaling for Analog Interfaces (LSSGR: アナログ インターフェイスのシグナリング)」に定義されているとおり、各 bellcore-dr 1-5 キーワードは標準の独自の呼び出しパターンをサポートしています。
手順 7	<code>exit</code> 例: Router(config-register-global)# exit	音声レジスタ グローバル コンフィギュレーション モードを終了します。
手順 8	<code>voice register pool tag</code> 例: Router(config)# voice register pool 20	SIP 電話の音声レジスタ プール コンフィギュレーション モードを開始します。 • このコマンドを使用して、Cisco Unified SIP SRST デバイスがどの電話登録を承認または拒否するかを制御できます。

	コマンドまたはアクション	目的
手順 9	<pre>no vad</pre> <p>例: Router(config-register-pool)# no vad</p>	<p>VoIP ダイアル ピアの音声アクティビティ検出(VAD)を無効にします。</p> <ul style="list-style-type: none"> VAD はデフォルトでは有効になっています。無音時にコンフォート ノイズがないため、コールは切断されたと見なされる場合があります。SIP 電話プールに no vad を設定した方が良い場合があります。
手順 10	<pre>codec codec-type [bytes]</pre> <p>例: Router(config-register-pool)# codec g729r8</p>	<p>Cisco Unified SIP SRST 環境内の単一の SIP 電話または VoIP ダイアル ピアによってサポートされるコーデックを指定します。<i>codec-type</i> 引数は、優先されるコーデックを指定します。次のいずれかになります。</p> <ul style="list-style-type: none"> g711alaw: G.711 A-law 64,000 bps g711ulaw: G.711 μ-law 64,000 bps g729r8: G.729 8000 bps (デフォルト) <p><i>bytes</i> 引数はオプションで、各フレームの音声ペイロードのバイト数を指定します。</p>
手順 11	<pre>end</pre> <p>例: Router(config-register-pool)# end</p>	<p>特権 EXEC モードに戻ります。</p>

SIP 間のコール転送の設定

SIP 間のコール転送(コールルーティング)を使用できます。コール転送は、電話によって、または任意のダイアル ピアでのコール転送を可能にするバックツーバック ユーザ エージェント (B2BUA) によって提供されます。SIP デバイスへのコールは、(Cisco Unity、サードパーティのボイスメールシステム、または IPCC や IPCC Express などの自動応答や IVR システムを含めて)他の SIP デバイスまたは SCCP デバイスに転送できます。さらに、SCCP IP 電話を SIP 電話に転送できます。

Cisco Unity または SIP トランクか SIP ユーザ エージェントによって接続されている他のボイスメッセージングシステムは、メッセージが残っている場合に、メッセージ待機インジケータ (MWI) を渡すことができます。その後、SIP 電話は、ボイスメッセージングシステムから指示されると、MWI を表示します。



(注)

SIP から H.323 へのコール転送はサポートされていません。

SIP 間のコール転送を設定するには、まず Cisco IP-IP ゲートウェイ内の特定のタイプのエンドポイント間での接続を許可する必要があります。**allow-connections** コマンドがこの機能を許可します。SIP 間の接続が許可されると、個々の SIP 電話プールの下でコール転送を設定できます。必要に応じて、次のコマンドのいずれかを使用して、コール転送を設定できます。

- voice register pool の下
 - call-forward b2bua all *directory-number*
 - call-forward b2bua busy *directory-number*
 - call-forward b2bua mailbox *directory-number*
 - call-forward b2bua noan *directory-number* [timeout seconds]

一般的な Cisco Unified SIP SRST 設定では、**call-forward b2bua mailbox** コマンドは使用されませんが、Cisco Unified SIP Communications Manager Express (CME) 環境では使用されるようです。**call-forward b2bua mailbox** コマンドの設定方法の詳細については、Cisco.com で [Cisco Unified Communications Manager \(CallManager\)](#) のドキュメントを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice register pool tag**
4. **call-forward b2bua all directory-number**
5. **call-forward b2bua busy directory-number**
6. **call-forward b2bua mailbox directory-number**
7. **call-forward b2bua noan directory-number timeout seconds**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
手順 1	enable 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	configure terminal 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	voice register pool tag 例: Router(config)# voice register pool 15	音声レジスタ プール コンフィギュレーション モードを開始します。 • このコマンドを使用して、Cisco Unified SIP SRST デバイスがどの電話登録を承認または拒否するかを制御できます。
手順 4	call-forward b2bua all directory-number 例: Router(config-register-pool)# call-forward b2bua all 5005	すべての着信コールを別の非 SIP ステーションの内線番号(つまり、SIP トランク、H.323 トランク、SCCP デバイスまたはアナログ/デジタル トランク)へ転送できるように、SIP バックツーバック ユーザ エージェント (B2BUA) のコール転送を有効にします。 • <i>directory-number</i> : コールの転送先電話番号。完全修飾された E.164 番号を表します。電話番号の最大長は 32 桁です。
手順 5	call-forward b2bua busy directory-number 例: Router(config-register-pool)# call-forward b2bua busy 5006	話中の内線番号への着信コールを別の内線番号に転送できるように、SIP B2BUA のコール転送を有効にします。 • <i>directory-number</i> : コールの転送先電話番号。完全修飾された E.164 番号を表します。電話番号の最大長は 32 桁です。

	コマンドまたはアクション	目的
手順 6	<pre>call-forward b2bua mailbox directory-number</pre> <p>例: Router(config-register-pool)# call-forward b2bua mailbox 5007</p>	<p>コール転送交換の最後にボイスメール システムで選択される特定のボイスメール ボックスを制御します。</p> <ul style="list-style-type: none"> directory-number: 転送された接続先が話中または応答しない場合のコールの転送先電話番号。完全修飾された E.164 番号を表します。電話番号の最大長は 32 桁です。
手順 7	<pre>call-forward b2bua noan directory-number timeout seconds</pre> <p>例: Router(config-register-pool)# call-forward b2bua noan 5010 timeout 10</p>	<p>設定された時間が経過しても応答のない内線番号への着信コールが別の内線番号へ転送されるように、SIP B2BUA のコール転送を有効にします。</p> <p>このコマンドは、電話が Cisco Unified SIP SRST ルータに登録されているが、IP 接続がないために電話が到達不能である (Invite 要求に応答しない) 場合に使用されます。</p> <ul style="list-style-type: none"> directory-number: コールの転送先電話番号。完全修飾された E.164 番号を表します。電話番号の最大長は 32 桁です。 timeout seconds: コールが別の内線番号に転送されるまで、無応答で呼び出すことができる期間 (秒単位)。範囲は 3 ~ 60000 です。デフォルト値は 20 です。
手順 8	<pre>end</pre> <p>例: Router(config-register-pool)# end</p>	<p>特権 EXEC モードに戻ります。</p>

時刻、曜日、または日付に基づくコールブロッキングの設定

このセクションの内容は、SCCP と SIP SRST の両方に適用されます。コールブロッキングは、電話の不正使用を防止し、指定の時刻、曜日、または日付に、最大 32 桁のパターンを一致させることで実装されます。Cisco Unified SIP SRST は、現在 SCCP 電話で提供されているものと同じ時間ベースのコールブロッキングメカニズムを SIP エンドポイントに提供します。コールブロッキング機能は、着信 SIP コールとアナログ FXS コールを含む、すべての着信コールをサポートします。



(注)

PIN ベースの免除および「ログイン」ツールバー オーバーライドは、Cisco Unified SIP SRST ではサポートされていません。

SIP 電話のコールブロッキングに使用されるコマンドは、Cisco Unified SRST システムの SCCP 電話で使用されるコマンドと同じです。Cisco SRST セッションアプリケーションは、call-manager-fallback モードで現在の時間外の設定にアクセスし、この設定を、Cisco SRST ルータに登録されている Cisco SIP Phone から発信されたコールに適用します。ブロックの基準 (時刻/日付/ブロックパターン) を設定する call-manager-fallback モードで使用されるコマンドは次のとおりです。

- **after-hours block pattern pattern-tag pattern [7-24]**
- **after-hours day day start-time stop-time**
- **after-hours date month date start-time stop-time**

コールブロッキングに定義された期間に、コールブロッキングに指定されたパターンと一致する桁にユーザが発信を試みると、コールは即座に終了され、発信者にはファストビジー音が聞こえます。

SRST (call-manager-fallback コンフィギュレーション モード) では、時間外のコールブロッキングに対する電話または PIN ベースの免除はありません。ただし、Cisco Unified SIP SRST (音声レジスタ プール モード) では、**after-hours exempt** コマンドを使用して、個々の IP Phone をすべてのコールブロッキングから免除することができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **call-manager-fallback**
4. **after-hours block pattern tag pattern [7-24]**
5. **after-hours day day start-time stop-time**
6. **after-hours date month date start-time stop-time**
7. **exit**
8. **voice register pool tag**
9. **after-hour exempt**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
手順 1	enable 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	configure terminal 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	call-manager-fallback 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。
手順 4	after-hours block pattern tag pattern [7-24] 例: Router(config-cm-fallback)# after-hours block pattern 1 91900	ブロックする発信桁のパターンを定義します。個別にコマンドを使用して、最大 32 のパターンを定義できます。 • 7-24 キーワードが指定された場合、パターンは、週 7 日、1 日 24 時間、常時ブロックされます。 • 7-24 キーワードが指定されていない場合は、パターンは after-hours day および after-hours date コマンドを使用して定義された日数および日付の間ブロックされます。

コマンドまたはアクション	目的
<p>手順 5 <code>after-hours day day start-time stop-time</code></p> <p>例: Router(config-cm-fallback)# after-hours day mon 19:00 07:00</p>	<p>after-hours block pattern コマンドを使用して定義された発信ダイヤルパターンへのコールがブロックされる曜日に基づいて、繰り返される期間を定義します。</p> <ul style="list-style-type: none"> <i>day</i>: 曜日の省略形。有効な曜日の省略形は、sun、mon、tue、wed、thu、fri、sat です。 <i>start-time stop-time</i>: コールブロッキングの開始時刻と終了時刻。HH:MM 形式の 24 時間制で指定します。停止時刻が開始時刻よりも早い時刻になっている場合、停止時刻は開始時刻の翌日になります。たとえば、「mon 19:00 07:00」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。 <p>値 24:00 は無効です。停止時刻に 00:00 を入力すると、23:59 に変更されます。開始時刻と停止時刻の両方に 00:00 を入力した場合、指定した日付の 24 時間全体でコールがブロックされます。</p>
<p>手順 6 <code>after-hours date month date start-time stop-time</code></p> <p>例: Router(config-cm-fallback)# after-hours date jan 1 00:00 00:00</p>	<p>after-hours block pattern コマンドを使用して定義された発信ダイヤルパターンへのコールがブロックされる月と日付に基づいて、繰り返される期間を定義します。</p> <ul style="list-style-type: none"> <i>month</i>: 月の省略形。有効な月の省略形は、jan、feb、mar、apr、may、jun、jul、aug、sep、oct、nov、dec です。 <i>date</i>: その月の日付。範囲は 1 ~ 31 です。 <i>start-time stop-time</i>: コールブロッキングの開始時刻と終了時刻。HH:MM 形式の 24 時間制で指定します。停止時刻は開始時刻よりも遅くする必要があります。 <p>値 24:00 は無効です。停止時刻に 00:00 を入力すると、23:59 に変更されます。開始時刻と停止時刻の両方に 00:00 を入力した場合、指定した日付の 24 時間全体でコールがブロックされます。</p>
<p>手順 7 <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>
<p>手順 8 <code>voice register pool tag</code></p> <p>例: Router(config)# voice register pool 12</p>	<p>音声レジスタ プール 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"> このコマンドは、どの登録が Cisco Unified SIP SRST デバイスによって承認または拒否されるかを制御するために使用します。
<p>手順 9 <code>after-hour exempt</code></p> <p>例: Router(config-register-pool)# after-hour exempt</p>	<p>特定の音声レジスタ プールの場合には、コールブロッキングが有効でも、発信コールを一切ブロックしないように指定します。</p>
<p>手順 10 <code>end</code></p> <p>例: Router(config-register-pool)# end</p>	<p>特権 EXEC モードに戻ります。</p>

例

次の例では、発信コールがブロックされる番号パターンをいくつか定義します。パターン 1 および 2 は、1 および 011 で始まる外部番号へのコールをブロックします。このブロックは、月曜日から金曜日の午前 7 時以前と午後 7 時以後に行われます。パターン 3 は、週 7 日、1 日 24 時間、900 番へのコールをブロックします。

```
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 day mon 19:00 07:00
after-hours day tue 19:00 07:00
after-hours day wed 19:00 07:00
after-hours day thu 19:00 07:00
after-hours day fri 19:00 07:00
```

次の例では、Cisco SIP 電話プールが設定されたブロッキング基準から免除されます。

```
voice register pool 1
after-hour exempt
```

検証

機能の設定を確認するには、次のコマンドのいずれかを入力します。

- **show voice register dial-peer**: 登録された電話によって動的に作成されたすべてのダイヤルピアを表示します。このコマンドは、時間外のブロッキングおよびコール転送の設定も表示します。
- **show voice register pool <tag>**: 特定のプールに関する情報を表示します。
- **debug ccsip messages**: 基本的な B2BUA コールをデバッグします。

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。

SIP のコール保留と保留解除

Cisco Unified SRST は、SIP 電話でコールを保留したり、コールの保留を解除したりする機能をサポートしています。これには、A が B にコールし、B が A を保留して、B が C にコールし、B が C から切断した後、A のコールを保留解除するコンサルティブ保留のサポートも含まれます。コール保留のサポートは、「re-INVITE c=0.0.0.0」を使用して SIP 電話によって、さらに受信専用メカニズムによっても示されます。

設定は不要です。

例

```
Router# show running-config
Building configuration...

Current configuration : 1462 bytes
configuration mode exclusive manual
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```



```
service internal
!
boot-start-marker
boot-end-marker
!
logging buffered 8000000 debugging
!
no aaa new-model
!
resource policy
!
clock timezone edt -5
clock summer-time edt recurring
ip subnet-zero
!
!
!
ip cef
!
!
!
voice-card 0
no dspfarm
!
!
voice service voip
  allow-connections h323 to h323
  allow-connections h323 to sip
  allow-connections sip to h323
  allow-connections sip to sip
sip
  registrar server expires max 600 min 60
!
!
!
voice register global
  max-dn 10
  max-pool 10
!
! Define call forwarding under a voice register pool
voice register pool 1
  id mac 0012.7F57.60AA
  number 1 1000
  call-forward b2bua busy 2413
  call-forward b2bua noan 2414 timeout 30

codec g711ulaw
!
voice register pool 2
  id mac 0012.7F3B.9025
  number 1 2800
  codec g711ulaw
!
voice register pool 3
  id mac 0012.7F57.628F
  number 1 2801
  codec g711ulaw
!
!
!
interface GigabitEthernet0/0
  ip address 10.0.2.99 255.255.255.0
  duplex auto
  speed auto
```

```

!
interface GigabitEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
!
ip http server
!
!
!
control-plane
!
!
!
dial-peer voice 1000 voip
  destination-pattern 24..
  session protocol sipv2
  session target ipv4:10.0.2.5
  codec g711ulaw
!
! Define call blocking under call-manager-fallback mode
call-manager-fallback
  max-conferences 4 gain -6
  after-hours block pattern 1 2417

                                after-hours date Dec 25 12:01 20:00
                                !
                                !
                                line con 0
                                exec-timeout 0 0
                                line aux 0
                                line vty 0 4
                                login
                                !
                                scheduler allocate 20000 1000
                                ntp server 10.0.2.10
                                !
                                end

```

オプション機能の設定方法

ここでは、次のオプションの追加コール機能について説明します。

- 3者間 G.711 アドホック会議: Cisco Unified Survivable Remote Site Telephony (SRST) は、同時3者間会議をサポートしています。
- 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。

次のセクションでは、これらの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 アドホック会議の有効化\(159 ページ\)](#)
- [XML API スキーマの定義\(160 ページ\)](#)

3 者間 G.711 アドホック会議の有効化

3 者間 G.711 アドホック会議を有効にするには、Cisco Unified SRST ルータによってサポートされる同時 3 者間会議の最大数を設定する必要があります。会議を使用するには、IP Phone に 1 つ以上のボタンに接続された 2 本以上の回線が必要です。[「2 次ダイヤルトーンの設定」セクション \(84 ページ\)](#)を参照してください。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 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。
手順 2	max-conferences <i>max-conference-numbers</i> 例: Router(config-cm-fallback)# max-conferences 16	ルータでサポートされる、同時 3 者間会議の最大数を設定します。可能な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"> • Cisco 1751 ルータ:8 • Cisco 1760 ルータ:8 • Cisco 2600 シリーズ ルータ:8 • Cisco 2600-XM シリーズ ルータ:8 • Cisco 2801 ルータ:8 • Cisco 2811、Cisco 2821、および Cisco 2851 ルータ:16 • Cisco 3640 および Cisco 3640A ルータ:8 • Cisco 3660 ルータ:16 • Cisco 3725 ルータ:16 • Cisco 3745 ルータ:16 • Cisco 3800 シリーズ ルータ:24
手順 3	exit 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、ルータに最大 8 件の同時 3 者間会議を設定しています。

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

XML API スキーマの定義

このセクションの Cisco IOS コマンドを使用して、XML API に関連付けられ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。設定手順については、『[Cisco SRST 3.0 で H.450.2 および H.450.3 を使用したコンサルタティブ コールの転送および自動転送の有効化](#)』セクション(133 ページ)を参照してください。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 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。
手順 2	xmlschema schema-url 例: Router(config-cm-fallback)# xmlschema http://server2.example.com/ schema/schema1.xsd	この Cisco Unified SRST システムで使用される XML API スキーマの URL を指定します。 • <i>schema-url</i> : RFC 2396 の定義に準じたローカルまたはリモート URL。
手順 3	exit 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。

コール処理の設定例

- 例: キー拡張モジュールのステータスのモニタリング(160 ページ)
- 例: Cisco Unified SIP SRST での音声ハント グループの設定(161 ページ)

例: キー拡張モジュールのステータスのモニタリング

show コマンドを使用して、キー拡張モジュール(KEM)のステータスおよびその他の詳細を監視します。

次の例は、**show voice register all** コマンドを使用して、Cisco Unified CME のすべての設定と登録の情報とともに KEM の詳細を表示する方法を示しています。

```
show voice register all
VOICE REGISTER GLOBAL
=====
CONFIG [Version=9.1]
=====
```

```

.....
Pool Tag 5
Config:
  Mac address is B4A4.E328.4698
  Type is 9971 addon 1 CKEM
  Number list 1 : DN 2
  Number list 2 : DN 3
  Proxy Ip address is 0.0.0.0
  DTMF Relay is disabled
  Call Waiting is enabled
  DnD is disabled
  Video is enabled
  Camera is enabled
  Busy trigger per button value is 0
  keep-conference is enabled
  registration expires timer max is 200 and min is 60
  kpml signal is enabled
  Lpcor Type is none

```

次の例は、**show voice register pool type** コマンドを使用して、アドオン KEM を設定したすべての電話機を Cisco Unified CME で表示する方法を示しています。

```

Router# show voice register pool type CKEM
Pool ID          IP Address      Ln DN  Number      State
=====
4      B4A4.E328.4698  9.45.31.111    1 4    5589$      REGISTERED

```

例: Cisco Unified SIP SRST での音声ハント グループの設定

次の例は、パイロット番号 4701、最後の番号 5000、およびリスト内の 6 個の番号を使用して、最長アイドルハントグループ 20 を設定する方法を示しています。コールが 6 回リダイレクトされると (6 回ホップが行われると)、最後の番号 5000 にリダイレクトされます。

```

Router(config)# voice hunt-group 20 longest-idle
Router(config-voice-hunt-group)# pilot 4701
Router(config-voice-hunt-group)# list 4001, 4002, 4023, 4028, 4045, 4062
Router(config-voice-hunt-group)# final 5000
Router(config-voice-hunt-group)# hops 6
Router(config-voice-hunt-group)# timeout 20
Router(config-voice-hunt-group)# exit

```

次の作業

セキュリティを設定する必要がある場合は、「[SCCP および SIP のセキュア SRST の設定](#)」セクション (163 ページ) を参照してください。また、ボイスメールを設定する必要がある場合は、「[ボイスメールと Cisco Unified SRST の統合](#)」セクション (243 ページ) を参照してください。ビデオパラメータを設定する必要がある場合は、「[ビデオパラメータの設定](#)」セクション (267 ページ) を参照してください。それらの機能のいずれも必要ない場合は、「[Cisco Unified SRST のモニタリングとメンテナンス](#)」セクション (281 ページ) に進んでください。

詳細については、「[Cisco Unified SRST 機能の概要](#)」セクション (1 ページ) の章の「[SCCP および SIP のセキュア SRST の設定](#)」セクション (163 ページ) を参照してください。

■ 次の作業



CHAPTER 8 SCCP および SIP のセキュア SRST の設定

セキュア SRST は、Cisco Unified SRST にセキュリティ機能を追加します。

目次

この章では、認証、保全性、およびメディア暗号化など、新しいセキュア SRST セキュリティ機能について説明します。

- [セキュア SRST を設定するための前提条件 \(163 ページ\)](#)
- [セキュア SRST の設定に関する制約事項 \(164 ページ\)](#)
- [セキュア SRST の設定について \(165 ページ\)](#)
- [セキュアな Unified SRST の設定方法 \(173 ページ\)](#)
- [その他の関連資料 \(223 ページ\)](#)
- [コマンド リファレンス \(224 ページ\)](#)
- [セキュア SCCP および SIP SRST の機能情報 \(224 ページ\)](#)
- [次の作業 \(225 ページ\)](#)

セキュア SRST を設定するための前提条件

一般

- セキュア SCCP および SIP SRST でサポートされているセキュア Cisco Unified IP Phone には、認証機関 (CA) またはサードパーティ証明書がインストールされている必要があります。暗号化が有効になっている必要があります。CA サーバ認証の詳細については、[CA サーバに対するセキュアな Cisco Unified SRST ルータの自動登録と認証 \(176 ページ\)](#) を参照してください。
- 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 認証局 (CA) 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。TLS チャンネル (ポート 2445) を介して、Unified SRST ルータと Cisco Unified Communications Manager の間で証明書の自動交換が行われます。ただし、Unified Communications Manager 経由での Unified SRST への電話機証明書交換は、Unified SRST ルータ上では手動でダウンロードする必要があります。
- Cisco Unified Communications Manager の証明書信頼リスト (CTL) が有効になっている必要があります。

セキュア SRST 上の Public Key Infrastructure (PKI)

- 手動または Network Time Protocol (NTP) 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有効にします。Public Key Infrastructure (PKI) 導入の詳細については、[Cisco IOS 証明書サーバに関する機能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の一部である場合、起動プロセスの間に次のメッセージが表示される場合があります。

```
% Failed to find Certificate Server's trustpoint at startup
% Failed to find Certificate Server's cert.
```

これらは情報メッセージであり、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ために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。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、これらのメッセージは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。

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

- セキュア 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、[Cisco Unified Survivable Remote Site Telephony の互換性情報](#)に関する機能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 12.1 のサポートされるファームウェア、プラットフォーム、メモリ、および音声製品機能](#)を参照してください。

セキュア SRST の設定に関する制約事項

一般

- 暗号化ソフトウェア機能 (「k9」) は、輸出が規制されています。この製品には、輸入、輸出、譲渡、使用を規制する米国またはその他の国の法律の対象となる暗号化機能が含まれています。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。

シスコの暗号化に関連する製品を管理す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/>

さらに詳しい情報が必要な場合は、`export@cisco.com` 宛てに電子メールでお問い合わせください。

- 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。

SCCP SRST

- セキュア SCCP 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。
- セキュア SCCP SRST は、Cisco 4000 シリーズ サービス統合型ルータではサポートされていません。

SIP SRST

- Cisco 4000 シリーズ サービス統合型ルータでは、セキュア SIP SRST のみがサポートされています。ルータ シリーズは、セキュア SCCP SRST をサポートしていません。
- SRTP パススルーはサポートされません。
- SDP パススルーはサポートされません。
- ビデオ コールはサポートされません。
- トランスコーディングはサポートされていません。
- ハードウェア会議はサポートされていません (BIB 会議のみがサポートされています)。
- **security-policy secure** を **voice register global** 設定モードの下に設定することは必須です。

セキュア SRST の設定について

- [セキュア SRST の利点\(165 ページ\)](#)
- [Cisco 4000 シリーズ サービス統合型ルータでのセキュア SRST サポート\(166 ページ\)](#)
- [非セキュア SRST での Cisco IP Phone のクリアテキスト フォールバック\(167 ページ\)](#)
- [Unified SRST でのシグナリングのセキュリティ\(TLS\)\(167 ページ\)](#)
- [Unified SRST でのメディアのセキュリティ\(SRTP\)\(169 ページ\)](#)
- [Cisco Unified IP Phone へのセキュアな Cisco Unified SRST の確立\(170 ページ\)](#)
- [セキュア SRST の認証および暗号化\(172 ページ\)](#)

セキュア SRST の利点

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セキュアな Cisco Unified 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 ルータはセキュア 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、セキュアなコール処理機能を再開します。

セキュア 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を使用すると、Cisco Unified 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。

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。
- セキュアなメディア パスが、Secure Real-Time Transport Protocol (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。

Cisco 4000 シリーズ サービス統合型ルータでのセキュア SRST サポート

Unified SRST 12.1 と以降のリリースでは、セキュア SIP SRST サポートは、Cisco 4000 シリーズ サービス統合型ルータに導入されました。Unified SRST リリース 12.1 のセキュア SIP SRST 機能の一部として、Transport Layer Security プロトコル (TLS) バージョン 1.2 までを使用するコールにサポートが提供されます。また、TLS 1.2 排他は、Unified SRST リリース 12.1 の一部としてサポートされます。

Cisco IP Phone 7800 シリーズおよび Cisco IP Phone 8800 シリーズは、Cisco 4000 シリーズ サービス統合型ルータ上で設定された Unified セキュア SIP SRST リリース 12.1 でサポートされます。

Cisco 4000 シリーズ サービス統合型ルータ上でサポートされるセキュア SIP SRST の場合、ルータ上で次の技術パッケージのライセンスを有効にする必要があります。

- セキュリティ
- uck9



(注)

セキュア SIP SRST の Cisco 4000 シリーズ サービス統合型ルータ上では、SIP 電話機のみがサポートされます。

セキュア保留音

Unified SRST リリース 12.1 から、セキュア保留音 (MOH) のサポートが、シスコ 4000 シリーズ サービス統合型ルータでのセキュア SIP SRST ソリューションの一部として導入されました。保留にされているセキュア SIP コールに対しては、Flash ベースの G.729 および G.711 コーデック形式 MOH ファイルの再生がサポートされています。ライブ MOH とトランスコードされた MOH は、セキュア MOH 機能サポートの一部としてはサポートされません。



(注)

CLI コマンド **srtp pass-thru** がダイヤルピア音声設定モードで設定されている場合、セキュア MOH は機能しません。

非セキュア 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 より前の Cisco Unified SRST バージョンでは、セキュア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 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。

Unified SRST でのシグナリングのセキュリティ (TLS)

- [SRST ルータおよび TLS プロトコル \(167 ページ\)](#)
- [セキュア SRST での証明書の操作 \(167 ページ\)](#)
- [CUCM からセキュア SRST への証明書の転送 \(169 ページ\)](#)

SRST ルータおよび TLS プロトコル

Transport Layer Security (TLS) バージョン 1.0 は、Cisco Unified IP Phone、セキュアな Cisco Unified SRST ルータ、および Cisco Unified Communications Manager の間にセキュアな TCP チャネルを提供します。TLS プロセスは、Cisco Unified Communications Manager への登録時に、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 とセキュアな Cisco Unified SRST ルータの間の 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。

Unified Secure SIP SRST リリース 12.1 から、Transport Layer Security (TLS) バージョン 1.2 までを使用する SIP 間コールのサポートが導入されました。TLS 1.2 排他機能を設定する場合、`sip-ua` 設定モードでコマンド `transport tcp tls v1.2` を設定する必要があります。セキュア SIP SRST に TLS 1.2 排他を設定する場合、他の TLS バージョンを使用した電話機による登録試行は拒否されます。

セキュア SRST での証明書の操作

- [Cisco Unified SRST ルータおよび PKI \(168 ページ\)](#)
- [セキュア SRST ルータの Cisco IOS クレデンシャル サーバ \(169 ページ\)](#)
- [クレデンシャル サーバの証明書の生成 \(169 ページ\)](#)

Cisco Unified SRST ルータおよび PKI

Cisco Unified SRST ルータと Cisco Unified Communications Manager の間での証明書の転送は、セキュア SRST 機能では必須です。Public Key Infrastructure (PKI) コマンドは、セキュアな 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 8-1 に、セキュア 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。「その他の関連資料」セクション(223 ページ)には、PKI コマンドを使用する証明書の生成、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、製造元でインストールされる証明書(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 LSC(ローカルで有効な証明書)の証明書を使用する、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 8-1 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、ローカルで有効な証明書(LSC)を認証局プロキシ機能(CAPF)から Distinguished Encoding Rules (DER)形式で受け取ります。</p> <ul style="list-style-type: none"> 59fe77ccd.0 <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、ローカルで有効な証明書(LSC)を認証局プロキシ機能(CAPF)から Distinguished Encoding Rules (DER)形式で受け取ります。</p> <ul style="list-style-type: none"> 59fe77ccd.0 <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される、製造元でインストールされる証明書(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"> CiscoCA.pem(証明書を認証するために使用される Cisco Root CA) <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"> a69d2e04.0(プライバシー強化メール(PEM)形式) <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>

セキュア SRST ルータの Cisco IOS クレデンシャル サーバ

セキュア SRST は、セキュア 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。セキュアな 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](#)

クレデンシャル サーバの証明書の生成

セキュアな Unified SRST でのクレデンシャル サーバの設定では、「**trustpoint <trustpoint name>**」設定エントリを完了するために証明書が必要です。

クレデンシャル サーバ用の証明書を生成するには、次の手順を実行します。

- [CA サーバに対するセキュアな Cisco Unified SRST ルータの自動登録と認証\(176 ページ\)](#)
- [セキュアな Cisco Unified SRST ルータでのクレデンシャル サービスの有効化\(181 ページ\)](#)
- [Cisco Unified Communications Manager での SRST フォールバックの設定\(192 ページ\)](#)

証明書が生成されたら、証明書の名前(または IOS のトラストポイントの名前)を「trustpoint」エントリに入力します。

セキュア SRST のクレデンシャル サーバ用のこの証明書は、「[Cisco Unified Communications Manager への SRST リファレンスの追加](#)」セクション(191 ページ)で要求されたときに Cisco Unified CM にシームレスにエクスポートされます。

CUCM からセキュア SRST への証明書の転送

CUCM からセキュア SRST への証明書の転送の詳細については、「[セキュアな 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](#)」セクション(183 ページ)を参照してください。

Unified SRST でのメディアのセキュリティ (SRTP)

Secure Real-Time Protocol (SRTP) を使用するメディア暗号化により、確実に、サポートされるデバイス間で目的の受信者のみがメディア ストリームを解釈できるようになります。サポートされているのは、音声ストリームだけです。

デバイスが SRTP をサポートしている場合、システムは SRTP 接続を使用します。1 つ以上のデバイスが SRTP をサポートしていない場合は、システムは RTP 接続を使用します。SRTP から RTP へのフォールバックは、セキュアなデバイスからセキュアではないデバイスへの保留音 (MOH) の転送などで発生する可能性があります。



(注) セキュア SRST では、異なるデバイスおよびプロトコルに応じて異なる方法でメディア暗号化キーが処理されます。SCCP を実行しているすべての電話機は、SRST からメディア暗号化キーを取得します。この場合、TLS 暗号化シグナリング チャネルによって電話機へのメディア暗号化キーのダウンロードが保護されます。SIP を実行している電話機は、自身のメディア暗号化キーを生成して保存します。SRST によって導出されたメディア暗号化キーは、暗号化されたシグナリング パス経由で、H.323 用の IPsec で保護されたリンクを介してゲートウェイに安全に送信されます。



警告

セキュリティ関連情報が暗号化されずに送信されないために Cisco H.323 ゲートウェイおよび H.323/H.245/H.225 トランクは IPsec 設定に依存しています。したがって、ゲートウェイおよびトランクに SRTP またはシグナリング暗号化を設定する前に、IPsec を設定することを強く推奨します。Cisco Unified SRST は、IPsec が正しく設定されていることを確認しません。IPsec を正しく設定しないと、セキュリティ関連情報が公開される可能性があります。

Cisco Unified IP Phone へのセキュアな Cisco Unified SRST の確立

図 8-1 に、SRST ルータ、Cisco Unified Communications Manager、および Cisco Unified IP Phone のクレデンシャル サーバのインターワーキングを示します。表 8-2 では、Cisco Unified IP Phone へのセキュア SRST の確立について説明します。

図 8-1 SRST ルータ、Cisco Unified Communications Manager、および Cisco Unified IP Phone のクレデンシャル サーバのインターワーキング

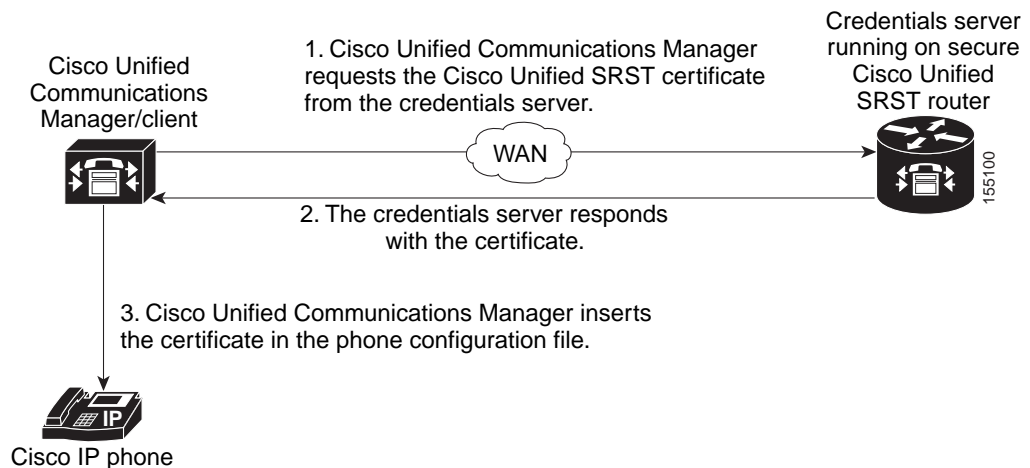


表 8-2 セキュア SRST の確立

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 Transport Layer Security (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、セキュアな Cisco Unified SRST ルータの情報および 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。 図 8-1 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。 図 8-1 を参照してください。 Cisco Unified Communications Manager が、セキュア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、セキュア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。	—

セキュア SRST の認証および暗号化

図 8-2 に、セキュア SRST の認証および暗号化のプロセスを示します。表 8-3 では、プロセスの内容について説明します。

図 8-2 セキュアな Cisco Unified SRST の認証および暗号化

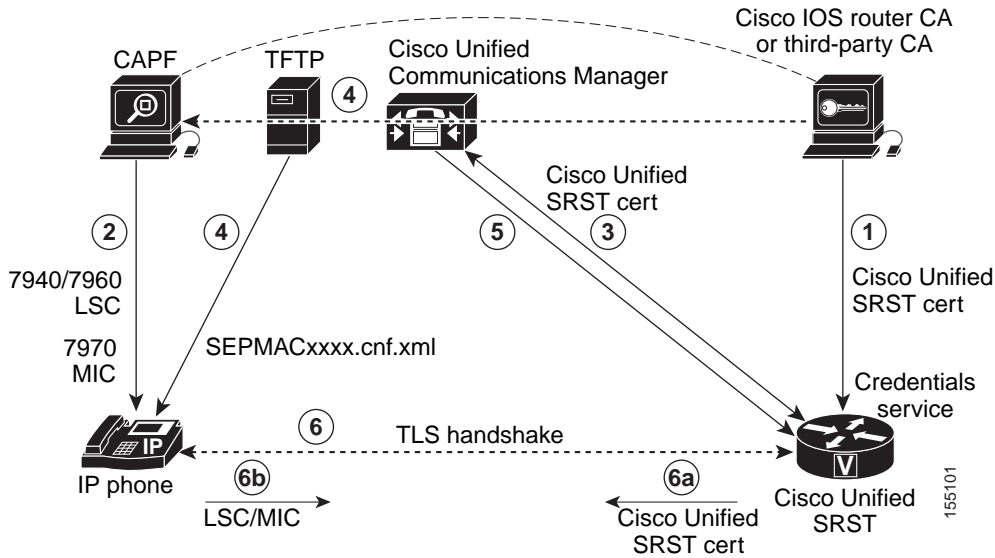


表 8-3 セキュア SRST の認証および暗号化プロセスの概要

プロセス手順	説明または詳細
1.	CA サーバが Cisco IOS ルータ CA またはサードパーティ CA であるかどうかにかかわらず、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。 CA ルータは、認証局プロキシ機能 (CAPF) の最終トラストポイントです。CAPF の詳細については、『 Cisco Communications Manager Security Guide 』を参照してください。
2.	CAPF は、サポートされているデバイスがローカルで有効な証明書 (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て、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。 LSC は、製造元でインストールされる証明書 (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。
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.	Cisco Unified CM はデバイスごとに 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。

表 8-3 セキュア SRST の認証および暗号化プロセスの概要(続き)

プロセス手順	説明または詳細
5.	<p>Cisco Unified CM 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、「セキュア SRST ルータの Cisco IOS クレデンシャル サーバ」セクション(169 ページ)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、電話機はステップ 4 で Cisco Unified CM 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、ステップ 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。

セキュアな Unified SRST の設定方法

設定に関する次のセクションでは、セキュアな 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 リンク障害の前後いずれにおいても、電話機が Cisco Unified SRST ルータに登録されるときに行われます。

ここでは、次の手順について説明します。

- [セキュア通信のための Cisco Unified SRST ルータの準備\(174 ページ\)](#)
- [セキュアな Cisco Unified SRST ルータへの Cisco Unified Communications Manager の設定\(191 ページ\)](#)
- [セキュアな Cisco Unified SRST ルータでの SRST モードの有効化\(194 ページ\)](#)
- [セキュア SCCP SRST の設定\(195 ページ\)](#)
- [Cisco SRST でのセキュアな SIP コールシグナリングおよび SRTP メディアの設定\(209 ページ\)](#)

セキュア通信のための Cisco Unified SRST ルータの準備

次の作業では、セキュア通信を行うために Cisco Unified SRST ルータを準備します。

- [Cisco IOS 証明書サーバでの認証局サーバの設定 \(174 ページ\)](#) (任意)
- [CA サーバに対するセキュアな Cisco Unified SRST ルータの自動登録と認証 \(176 ページ\)](#) (必須)
- [自動証明書登録の無効化 \(178 ページ\)](#) (必須)
- [証明書登録の確認 \(179 ページ\)](#) (任意)
- [セキュアな Cisco Unified SRST ルータでのクレデンシャル サービスの有効化 \(181 ページ\)](#) (必須)
- [クレデンシャル設定のトラブルシューティング \(182 ページ\)](#)
- [セキュアな 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 \(183 ページ\)](#)

Cisco IOS 証明書サーバでの認証局サーバの設定

Cisco Unified SRST ルータがセキュア通信を提供するには、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 ルータまたは別の 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手順の詳細については、[Cisco IOS 証明書サーバ](#)のマニュアルを参照してください。次に、設定例を示します。

手順の概要

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`

手順の詳細

	コマンドまたはアクション	目的
手順 1	<pre>crypto pki server cs-label</pre> <p>例: Router (config)# crypto pki server srstcaserver</p>	<p>証明書サーバを有効にし、証明書サーバ コンフィギュレーション モードを開始します。</p> <p>(注) 手動で RSA キー ペアを生成した場合、<i>cs-label</i> 引数はキー 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、Cisco IOS 証明書サーバのマニュアルを参照してください。</p>
手順 2	<pre>database level {minimal names complete}</pre> <p>例: Router (cs-server)# database level complete</p>	<p>証明書登録データベースに保管されるデータのタイプを制御します。</p> <ul style="list-style-type: none"> • minimal: 新しい証明書を、継続して問題なく発行できる程度の情報が保管されます。これがデフォルト値です。 • names: minimal レベルで提供される情報以外に、各証明書のシリアル番号および所有者名を保存します。 • complete: minimal レベルおよび names レベルで提供される情報以外に、発行済みの各証明書がデータベースに書き込まれます。 <p>(注) complete キーワードを指定すると、大量の情報が生成されます。このキーワードを発行する場合、database url コマンドを使用して、データを保管する外部 TFTP サーバも指定する必要があります。</p>
手順 3	<pre>database url root-url</pre> <p>例: Router (cs-server)# database url nvram</p>	<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。crypto pki server 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"> • 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。
手順 4	<pre>issuer-name DN-string</pre> <p>例: Router (cs-server)# issuer-name CN=srstcaserver</p>	<p>指定した識別名 (DN-string) に CA 発行者名を設定します。デフォルト値は次のとおりです。</p> <p>issuer-name CN=cs-label.</p>
手順 5	<pre>grant auto</pre> <p>例: Router (cs-server)# grant auto</p>	<p>あらゆる要求者に対して証明書が自動的に発行されるようにします。</p> <ul style="list-style-type: none"> • このコマンドは登録時にのみ使用され、「自動証明書登録の無効化」セクション (178 ページ) で削除されます。
手順 6	<pre>no shutdown</pre> <p>例: Router (cs-server)# no shutdown</p>	<p>Cisco IOS 証明書サーバを有効にします。</p> <ul style="list-style-type: none"> • このコマンドは、証明書サーバの設定が完了した後で発行する必要があります。

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 サーバに対するセキュアな Cisco Unified SRST ルータの自動登録と認証

セキュアな 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、セキュアな Cisco Unified SRST ルータはセキュア SRST ルータとして Cisco Unified Communications Manager に認識されます。

CA サーバにセキュアな 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。コマンドの使用手順の詳細については、[証明機関相互運用性コマンド](#)のマニュアルを参照してください。自動登録の例は、[証明書登録拡張機能](#)で入手できます。「例」セクション(178 ページ)に、設定例を示します。

手順の概要

1. **crypto pki trustpoint** *name*
2. **rsa***keypair* *keypair-label*
3. **enrollment url** *url*
4. **revocation-check** *method1*
5. **exit**
6. **crypto pki authenticate** *name*
7. **crypto pki enroll** *name*

手順の詳細

	コマンドまたはアクション	目的
手順 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 CA を宣言し、CA トラストポイント 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"> 指定される名前は、「セキュアな Cisco Unified SRST ルータでのクレデンシャル サービスの有効化」セクション(181 ページ)で宣言されるトラストポイント名と同じになります。
手順 2	<pre>rsaakeypair keypair-label</pre> <p>例: Router(config-trustp)# rsaakeypair srstcakey 2048</p>	<p>このトラストポイントに対して名前付きの Rivest, Shamir, and Adelman (RSA) キー ペアを指定するには、トラストポイント コンフィギュレーション モードで rsaakeypair コマンドを使用します。</p> <ul style="list-style-type: none"> TLS 1.2 バージョンでは、RSA キーの長さは 2048 ビットに設定されています。
手順 3	<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"> url url: ルータが認証要求を送信する CA の URL を指定します。 登録にシスコ独自の SCEP を使用している場合、url は <code>http://CA_name</code> という形式にする必要があります。ここで、<i>CA_name</i> は、Cisco IOS CA のホストドメイン ネーム システム (DNS) 名または IP アドレスです。 「Cisco IOS 証明書サーバでの認証局サーバの設定」セクション(174 ページ)に記載されている手順を使用した場合、URL は、ステップ 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 を使用した場合、IP アドレスは外部 CA になります。
手順 4	<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。<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、証明書が常に承認されることを意味します。</p> <ul style="list-style-type: none"> この作業では、none キーワードを使用することが必須です。
手順 5	<pre>exit</pre> <p>例: Router(ca-trustpoint)# exit</p>	<p>CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。</p>
手順 6	<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"> CA の名前を引数として指定します。
手順 7	<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"> CA の名前を引数として指定します。

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: DOB9E79C
% 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、「[Cisco IOS 証明書サーバでの認証局サーバの設定](#)」セクション(174 ページ)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) 証明書が継続的に供与されないように、**grant auto** コマンドを無効にする必要があります。

手順の概要

1. **crypto pki server cs-label**
2. **shutdown**
3. **no grant auto**
4. **no shutdown**

手順の詳細

	コマンドまたはアクション	目的
手順 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、証明書サーバ コンフィギュレーション モードを開始します。 (注) 手動で RSA キー ペアを生成した場合、 <i>cs-label</i> 引数はキー ペアの名前と一致する必要があります。
手順 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。
手順 3	<code>no grant auto</code> 例: Router (cs-server)# <code>no grant auto</code>	あらゆる要求者に対する証明書の自動発行を無効にします。 • 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。
手順 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。 • このコマンドは、証明書サーバの設定が完了した後に発行する必要があります。

次の作業

手動登録の手順については、[証明書手動登録 \(TFTP およびカット アンド ペースト\)](#) 機能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。

手順の概要

1. `show running-config`
2. `show crypto pki server`

手順の詳細

	コマンドまたはアクション	目的
手順 1	<pre>show running-config 例: 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 9B8355EE C10F8963</pre>	<p>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。</p>

	コマンドまたはアクション	目的
	<pre> 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 </pre>	
手順 2	<pre> show crypto pki server 例: 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 </pre>	<p>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。</p>

セキュアな 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 はセキュアな 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有効化します。



(注)

セキュリティ上のベストプラクティスは、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、[コントロールプレーンポリシングのマニュアル](#)を参照してください。また、「[コントロールプレーンポリシング:例](#)」セクション(208 ページ)に設定例を示します。

手順の概要

1. **credentials**
2. **ip source-address** *ip-address* [**port** *port*]
3. **trustpoint** *trustpoint-name*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
手順 1	credentials 例: Router(config)# credentials	Cisco Unified SRST ルータの証明書を Cisco Unified Communications Manager に提供し、クレデンシアル コンフィギュレーション モードを開始します。
手順 2	ip source-address <i>ip-address</i> [port <i>port</i>] 例: Router(config-credentials)# ip source-address 10.1.1.22 port 2445	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"> • ip-address: 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。 • port port: (任意) 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。
手順 3	trustpoint <i>trustpoint-name</i> 例: Router(config-credentials)# trustpoint srstca	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。 <i>trustpoint-name</i> 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"> • トラストポイント名は、「CA サーバに対するセキュアな Cisco Unified SRST ルータの自動登録と認証」セクション(176 ページ)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。
手順 4	exit 例: Router(config-credentials)# exit	クレデンシアル 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
```

クレデンシアル設定のトラブルシューティング

次の手順では、クレデンシアル設定を表示するか、Cisco Unified SRST ルータのクレデンシアル設定のデバッグを設定します。

手順の概要

1. **show credentials**
2. **debug credentials**

手順の詳細

	コマンドまたはアクション	目的
手順 1	show credentials 例: <pre>Router# show credentials Credentials IP: 10.1.1.22 Credentials PORT: 2445 Trustpoint: srstca</pre>	セキュアな 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。
手順 2	debug credentials 例: <pre>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.</pre>	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。

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、ルータが電話機の認証に使用した証明書がわかります)。

- `debug crypto pki messages`
- `debug crypto pki transactions`

セキュアな 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 Unified IP Phone に必要な作業を完了して、セキュア SRST を認証します。

Cisco Unified Communications Manager 4.X.X 以前のバージョン

Cisco Unified Communications Manager 4.X.X 以前のバージョンを実行しているシステムの場合、セキュアな 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 8-1 に、電話機のタイプごと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。手動登録の手順については、[証明書手動登録 \(TFTP およびカット アンド ペースト\)](#)機能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 4.X.X 以前のバージョンの場合、Cisco Unified Communications Manager のメニューバーで、[プログラム ファイル (Program Files)] > [Cisco] > [証明書 (Certificates)] を選択することで、証明書を検索できます。

Windows ワードパッドまたはメモ帳を使用して .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 Operating System Administration Guide, Release 6.1(1)』に記載されている認定操作については、http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cucos/6_1_1/cucos/iptpch6.html を参照してください。

Cisco Unified Communications Manager 5.0 以降のバージョン

Cisco Unified CM 5.0 以降のバージョンを実行しているシステムには、[表 8-1](#) に示されている要件に加えて、4 つの証明書 (CAPF、CiscoCA、CiscoManufactureCA、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 CM 5.0 以降のバージョンの場合、次の手順を実行します。

-
- 手順 1 Cisco Unified Communications Manager にログインします。
 - 手順 2 [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] > [証明書/CTL のダウンロード (Download Certificate/CTL)] に進みます。
 - 手順 3 [信頼証明書のダウンロード (Download Trust Cert)] を選択し、[次へ (Next)] をクリックします。
 - 手順 4 [CAPF 信頼 (CAPF-trust)] を選択し、[次へ (Next)] をクリックします。
 - 手順 5 [CiscoCA] を選択し、[次へ (Next)] をクリックします。
 - 手順 6 [続行 (Continue)] をクリックします。
 - 手順 7 ファイル名をクリックします。

- 手順 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。
- 手順 9 CiscoManufactureCA、CiscoRootCA2048、および CAPF に対して、ステップ 5～8 を繰り返します。

Cisco Unified Communications Manager 6.0 以降のバージョン

Cisco Unified Communications Operating System Administration から、[CAPF 信頼 (CAPF-trust)] の下にリストされているすべての証明書 (Cisco_Manufacturing_CA、Cisco_Root_CA_2048、CAP-RTP-001、CAP-RTP-002、CAPF、CAPF-xxx など) をダウンロードします。また、[CAPF 信頼 (CAPF-trust)] の下にはなく [CallManager 信頼 (CallManager-trust)] の下にリストされているすべての CAPF-xxx 証明書もダウンロードします。

証明書のダウンロード手順については、適切なバージョンの『[Cisco Unified Communications Operating System Administration Guide](#)』の「Security」の章を参照してください。

Cisco Unified SRST ルータでのインポートされた証明書の認証

Cisco Unified SRST ルータで証明書を認証するには、次の手順を実行します。

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。

手順の概要

1. `crypto pki trustpoint name`
2. `revocation-check none`
3. `enrollment terminal`
4. `exit`
5. `crypto pki authenticate name`

手順の詳細

	コマンドまたはアクション	目的
手順 1	<code>crypto pki trustpoint name</code> 例: Router (config)# <code>crypto pki trustpoint CAPF</code>	ルータが使用する CA を宣言し、CA トラストポイント 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"> • <i>name</i>: 各証明書の名前を個別に入力します (たとえば、CAPF、CiscoCA、CiscoManufactureCA、CiscoRootCA2048)。
手順 2	<code>revocation-check none</code> 例: Router(ca-trustpoint)# <code>revocation-check none</code>	選択した方法を使用して、証明書の失効ステータスをチェックします。 <ul style="list-style-type: none"> • この作業では、none キーワードを使用することが必須です。none キーワードは、失効チェックが実行されず、証明書が常に承認されることを意味します。

	コマンドまたはアクション	目的
手順 3	<code>enrollment terminal</code> 例: Router(ca-trustpoint)# <code>enrollment terminal</code>	カットアンドペーストによる手動での証明書登録を指定します。
手順 4	<code>exit</code> 例: Router(ca-trustpoint)# <code>exit</code>	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
手順 5	<code>crypto pki authenticate name</code> 例: Router(config)# <code>crypto pki authenticate CAPF</code>	CA から証明書を取得することにより、CA を認証します。 • 手順 1 において <code>crypto pki trustpoint</code> コマンドで使用したのと同じ <code>name</code> 引数を入力します。

次の作業

Cisco Unified CM の証明書を更新します。適切なバージョンの『[Cisco Unified Communications Manager Security Guide](#)』の「Configuring a Secure Survivable Remote Site Telephony (SRST) Reference」の章を参照してください。

例

ここで紹介する例は、次のとおりです。

- [Cisco Unified Communications Manager 4.X.X 以前のバージョンの例 \(186 ページ\)](#)
- [Cisco Unified Communications Manager 5.0 以降のバージョンの例 \(189 ページ\)](#)

Cisco Unified Communications Manager 4.X.X 以前のバージョンの例

次の例は、Cisco Unified SRST ルータにインポートされた 3 つの証明書 (Cisco 7970、7960、PEM) 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
MIIDqDCCApCgAwIBAgIQNT+yS9cPFKNGwfOprHJWdTANBqkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwTDQVAtU1RQLTAwMjAe
Fw0wMzEwMTAyMDE4NDlaFw0yMzEwMTAyMDI3MzdaMC4xFjAUBGNVBAoTDUNpc2Nv
IFN5c3RlbXMxZDASBgNVBAMTC0NBUC1SVFAtMDAyMIIIBIDANBgkqhkiG9w0BAQEF
AAOCAQ0AMIIBCjCAQEAxwZlBk19w/2NZVVvpjCPrpW1cCY7V1q9lhZl85RZZdnQ
2M4CufgIzNa3zYxGJIAYeFfcREcNMB3f5A+x7xNiEuzE87UPvK+7S80uWCY0Uhtl
AVVf5NqgZ3YDNoNXg5MmONb8lT86F55EzyVac0XGne77TSIbIdejrTgYXGP2MJX
Qhg+ZQlGFDRzbHfM84Duv2Msez+l+SqmQ080kIckqE9Nr3/XCSjlhXZNNVg8D+mv
Hth2P6KZqAKXAAsTGRLSZX3jNbS8tveJ3Gi5+sJ9+F6KKK2PD0iDwHcRKkcUHb7g
lI++U/5nswjUDIaph715Ds2rn9ehkMGipGLF8kpuCwIBA6OBwzCBwDALBgNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUUpIr4ojuLgmKTn5wLFal
mrTUm5YwbwYDVR0fBGgwZjBkoGKgYIYtAHR0cDovL2NhcC1ydHAtdMDAyL0NlcnRf
bnJvbGwvQ0FQLVJlUUC0wMDIuY3Jshi9maWx1Oi8vXFxjYXAtcnRwLTAwMlxzDZXJ0
RW5yb2xsXENBUCLSVFAtMDAyLmNybDAQBgkrBgEAAI3FQEEAwIBADANBgkqhkiG
9w0BAQUFAAOCAQEAVoOM78TaOtHqj7sVL/5u5VChlyvU168f0piJLWip2vDRihm
E+DlXdWMS5JaquTuaSd/m/xzxpCRJm4ZRRwPq6VeaiiQGkjFuZE5jSKiSAK7eHg
```



```
c6Ea7fm53nQRlcSPmUVLjDBzKYDNbnEjizptaIC5fgB/S9S6C1q0YpTZFn5tjUjy
WXzeYSXPrxcb0UH7IQJlogpONAAUKLoPaZU7tVDSH3hD4+VjmLyysaLUhksGFrrN
phzZrsVVilK17qpqCPl1KLGAS4fSbkruq3r/6S/SpXS6/gAoljBKixP7ZW2PxgCU
1aU9cURLPO95NDOFN3jBk3Sips7cVidcogowPQ==
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
```

Use the **show crypto pki trustpoint status** command to show that enrollment has succeeded and that five CA certificates were granted. The five certificates include the three certificates just entered and the CA server certificate and the SRST router certificate.
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 3A8E7DC7
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 以降のバージョンの例

次の例は、Cisco Unified Communications Manager 5.0 を実行するシステムに必要な 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
GjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMgSW5jMRYwFAYDVQQDEw1DQVBGLTU4RUFEMkQy
MkQyMB4XDTA2MDMwMTIxMjc1MloXDTEyMDIyNTIxMjc1MVowQTElMAkGA1UEBhMC
VVMxGjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMgSW5jMRYwFAYDVQQDEw1DQVBGLTU4
RUFEMkQyMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC99KgZT94qhozW4bOB
f8Z0tYwT2l4L++mC6403s3AshDi8xe8Y8sN/f/ZKRrhNixB1K4SwafXnHKJBqKZn
WtSgkRjJ3Dh0XtqcWYt8VS2sC69g8sX09lSkK13m+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
MIIDqDCCApCgAwIBAgIQdhL5YBU9b590QiAgMrcjVjANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEw1DQVAtU1RQLTAwMTAe
Vd54qlpc/hQDfWlbrIFkCcYhHws7vwnPsLuy1Kw2L2cP0UXxYghSsx8H4vGqdPFQ
NnYy7aKJ43SvDFt4zn37n8jrvlRuz0x3mdbcBEHbA825Yo7a8sk12tshMJ/YdMm
vny0pmDNZxmeHjqEgV03UFUN6GVC0+K1y1dUU1qpYJNYtqLkqj7wgccGjsHdHr3a
U+bwluLgSGsQnxMWeMaWo8+6hMxw1ANPweufgZMaywIBA6OBwzCBwDALBgNVHQ8E
c6Ea7fm53nQR1cSPmUVLjDBzKYDNbnEjizptaIC5fgB/S9S6C1q0YpTZFn5tjUjy
WXzeYSXPrxcb0UH7IQJlogpONAAUKLoPaZU7tVDSH3hD4+VjmLyysaLÜhksGFrrN
phzZrsVvilk17qpqCPllKLGAS4fSbkruq3r/6S/SpXS6/gAoljBKixP7ZW2PxxGCU
1aU9cURLPO95NDOFN3jBk3Sips7cVidcogowPQ==
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/g2qqfEMkHFp68dGf/2c5k5WnNnYhMODR9elXBSZBcG7FncXNtq6jUAQQIBA6OC
AecwggHjMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFNDFIiarT0Zg7K4F
kcfWtGwR/dsMAsGA1UdDQEAwIBhjAQBgkrBgEEAYI3FQEEAwIBADAZBgkrBgEE
AYI3FAIEDB4KAFMAdQBiAEMAQTAfBgNVHSMEGDAWgBQn88gVHm6aAgkWrSugiWBf
2nsvqjBDBgNVHR8EPDA6MDiqNqA0hjJodHRwOi8vd3d3LmNpc2NvLmNvbS9zZWY1
cm10eS9wa2kvY3JsL2NyY2EyMDQ4LmNyY2EybDBggrBgEFBQcBAQREMEIwQAYIKwYB
BQUHMAKGNGh0dHA6Ly93d3cuY2lyZ28uY29tL3L3NyY28uY29tL3L3NyY28uY29tL3L3
cmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkVAQIAMEMwQQYIKwYBBQUH
I+ii6itvaSN6go4cTANPpE+rhC836WVg0ZrG2PML9d7QJwBcbx2RvdFOWFEdyeP3
OOofTCrFovo4ipUsG4eakqjN9GnW6JvNwxmEapcN5JlunGdGTjaubEBEPH6GC/f08
S25l3JNFbemvM2tnIwcGhiLa69yHzlkhQhrpz3B1iOAKPV19Tpy4gJFVb/Cbcedi6
YBmlsGGGrd1lZva5J6LuL2GbuqEwYf2+rDUU+bgtlwavw+9tzD0865XpgdOKXrbo
+nmka9eiv2TEP0zJ2+ic7AFm1BCIo1blPFft6QKoSjFjB6thJksaE5/k3Npf
quit
Certificate has the following attributes:
Fingerprint MD5: 0F3BA6B7 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
MRYwFAYDQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDEwJDAXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWncNMDQwNTE0MjAxNTQyWjA1MRYwFAYDQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDEwJDAXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFbi71R803UXHojgkxkLtv5MOhmBvrbW7hmW
Yqpa02TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJt37mjpXYgyC81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YARetIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEblfJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX41Id
kxpUnwVvwEpxYB5DC2Ae/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

```

セキュアな 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\(191 ページ\)](#) (必須)
- [Cisco Unified Communications Manager での SRST フォールバックの設定\(192 ページ\)](#) (必須)
- [Cisco Unified Communications Manager での CAPF の設定\(193 ページ\)](#) (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、「[セキュアな Cisco Unified SRST ルータでのクレデンシャル サービスの有効化](#)」セクション(181 ページ)を参照してください。

Cisco Unified Communications Manager への Cisco Unified SRST の追加の詳細については、実行している Cisco Unified Communications Manager バージョンの「Survivable Remote Site Telephony Configuration」のセクションを参照してください。すべての Cisco Unified CM 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 にあります。

-
- 手順 1 Cisco Unified Communications Manager のメニュー バーで、[CCMAdmin] > [システム(System)] > [SRST] を選択します。
 - 手順 2 [新規 SRST リファレンスの追加(Add New SRST Reference)] をクリックします。
 - 手順 3 適切な設定値を入力します。[図 8-3](#) に、[SRST リファレンスの設定(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 ゲートウェイがセキュア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 8-3 [SRST リファレンスの設定 (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

127020

- 手順 4 新しい SRST リファレンスを追加するには、[挿入 (Insert)] をクリックします。「ステータス:挿入が完了しました (Status: Insert completed)」メッセージが表示されます。
- 手順 5 さらに SRST リファレンスを追加するには、ステップ 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 プールの Cisco Unified Communications Manager への追加の詳細については、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」のセクションを参照してください。すべての Cisco Unified CM アドミニストレーションガイドは、http://www.cisco.com/en/US/products/sw/voicew/sw556/prod_maintenance_guides_list.html にあります。

- 手順 1 Cisco Unified Communications Manager のメニュー バーで、[CCMAdmin] > [システム (System)] > [デバイス プール (Device Pool)] を選択します。
- 手順 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、[コピー (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。手順 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、手順 3 に進みます。

- 手順 3 ウィンドウの右上隅で、[新規 デバイス プールの追加 (Add New Device Pool)] リンクをクリックします。[デバイス プール設定 (Device Pool Configuration)] ウィンドウが表示されます(図 8-4 を参照)。

図 8-4 [デバイス プール設定 (Device Pool Configuration)] ウィンドウ

The screenshot shows the Cisco CallManager Administration interface for configuring a Device Pool. The main heading is "Device Pool Configuration". Below it, the current device pool is identified as "Default (13 members)**" with a status of "Ready". There are buttons for "Copy", "Update", "Delete", and "Reset Devices". The "Device Pool Settings" section includes various dropdown menus: Device Pool Name* (Default), Cisco CallManager Group* (Default), Date/Time Group* (CMLocal), Region* (Default), Softkey Template* (Standard User), SRST Reference* (jaso2691), Calling Search Space for Auto-registration (— Not Selected —), Media Resource Group List (jaso2691), Network Hold MOH Audio Source (SRST GW), User Hold MOH Audio Source (< None >), and Network Locale (< None >). The SRST Reference dropdown is currently expanded, showing options: — Not Selected —, Disable, Use Default Gateway, jaso2691 (highlighted), and SRST GW. The Cisco Systems logo is in the top right corner.

- 手順 4 SRST リファレンスを入力します。
- 手順 5 [更新(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 での CAPF の設定

認証局プロキシ機能 (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 に LSC 証明書を要求できます。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ます。

Cisco Unified Communications Manager の CAPF の設定の詳細については、『[Cisco IP Phone Authentication and Encryption for Cisco Communications Manager](#)』を参照してください。

セキュアな 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セキュア SRST を設定するには、グローバル 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。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
手順 1	call-manager-fallback 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。
手順 2	secondary-dialtone <i>digit-string</i> 例: Router(config-cm-fallback)# secondary-dialtone 9	<i>digit-string</i> がダイヤルされたときに、2 次ダイヤル トーンをアクティブにします。
手順 3	transfer-system { blind full-blind full-consult local-consult } 例: Router(config-cm-fallback)# transfer-system full-consult	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。 <ul style="list-style-type: none"> • blind: 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。 • full-blind: 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。 • full-consult: 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 full-blind にフォールバックします。 • local-consult: 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 blind にフォールバックします。
手順 4	ip source-address <i>ip-address</i> [port <i>port</i>] 例: Router(config-cm-fallback)# ip source-address 10.1.1.22 port 2000	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。

	コマンドまたはアクション	目的
手順 5	<code>max-ephones max-phones</code> 例: Router(config-cm-fallback)# max-ephones 15	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、「 プラットフォームとメモリのサポート 」セクション (26 ページ) を参照してください。
手順 6	<code>max-dn max-directory-numbers</code> 例: Router(config-cm-fallback)# max-dn 30	ルータがサポートできる電話番号 (DN) または仮想音声ポートの最大数を設定します。 <ul style="list-style-type: none"> <code>max-directory-numbers</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。詳細については、「プラットフォームとメモリのサポート」セクション (26 ページ) を参照してください。
手順 7	<code>transfer-pattern transfer-pattern</code> 例: Router(config-cm-fallback)# transfer-pattern	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。 <ul style="list-style-type: none"> <code>transfer-pattern</code>: 許可されるコール転送の数字列。ワイルドカードを使用できます。
手順 8	<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
```

セキュア SCCP SRST の設定

- [セキュア SCCP SRST を設定するための前提条件 \(195 ページ\)](#)
- [セキュア SCCP SRST の設定に関する制約事項 \(196 ページ\)](#)
- [電話機のステータスおよび登録の確認 \(196 ページ\)](#) (必須)
- [セキュア SCCP SRST の設定例 \(203 ページ\)](#)

セキュア SCCP SRST を設定するための前提条件

- Cisco Unified Communications Manager 4.1(2) 以降がインストールされ、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。

セキュア SCCP SRST の設定に関する制約事項

セキュア SCCP SRST モードではサポートされない

- Cisco Unified Communications Manager 4.1(2) 以前のバージョン
- セキュアな MOH (MOH はアクティブのままであるが非セキュアに戻る)
- セキュアなトランスコーディングまたは電話会議
- セキュアな H.323 または SIP トランク
- SIP 電話の相互運用性
- [Hot Standby Router Protocol \(HSRP\)](#)

セキュア SCCP SRST モードでサポートされるコール

セキュア SCCP SRST モードでは音声コールのみがサポートされます。具体的には、次の音声コールがサポートされます。

- 基本的なコール
- コール転送 (コンサルタティブ、ブラインド)
- コール自動転送 (話中、無応答時、不在転送)
- 共有回線 (IP Phone)
- 保留と復帰

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。



(注)

次の手順を実行した後に、セキュア SCCP SRST の電話機のステータスおよび登録を確認できます。

- [セキュアな Cisco Unified SRST ルータでのクレデンシャルサービスの有効化 \(181 ページ\)](#)
- [Cisco Unified Communications Manager への SRST リファレンスの追加 \(191 ページ\)](#)
- [セキュアな Cisco Unified SRST ルータでの SRST モードの有効化 \(194 ページ\)](#)

手順の概要

1. `show ephone`
2. `show ephone offhook`
3. `show voice call status`
4. `debug ephone register`
5. `debug ephone state`

手順の詳細

コマンドまたはアクション	目的
<p>手順 1 <code>show ephone</code></p> <p>例: Router# <code>show ephone</code></p> <pre>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</pre>	<p>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、セキュア SCCP 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。</p>
<p>手順 2 <code>show ephone offhook</code></p> <p>例: Router# <code>show ephone offhook</code></p> <pre>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</pre>	<p>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セキュア コールが存在します。</p>

■ セキュアな Unified SRST の設定方法

コマンドまたはアクション	目的
<pre>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</pre>	

	コマンドまたはアクション	目的
手順 3	<pre>show voice call status</pre> <p>例:</p> <pre>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 0x8608DC20 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 0x860E4008 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</pre>	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 ダイアルピア間のコールには適用できません。

■ セキュアな Unified SRST の設定方法

コマンドまたはアクション	目的
<pre>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</pre>	
<p>手順 4 debug ephone register</p> <p>例:</p> <pre>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</pre>	<p>Cisco IP Phone の登録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。</p>

	コマンドまたはアクション	目的
手順 5	<pre>debug ephone state 例: 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]:---SkinnySyncPhoneDnOverlay s 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</pre>	<p>2つのセキュアな 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。</p>

コマンドまたはアクション	目的
<pre> *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]:---SkinnySyncPhoneDnOverlay s 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 </pre>	

コマンドまたはアクション	目的
<pre>*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</pre>	

セキュア SCCP SRST の設定例

ここでは、次の設定例を示します。

- [セキュア SCCP SRST:例\(203 ページ\)](#)
- [コントロールプレーン ポリシング:例\(208 ページ\)](#)



(注) 例に示す IP アドレスおよびホスト名は架空のものです。

セキュア SCCP SRST:例

ここでは、前のセクションで説明した設定作業に対応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 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
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 EA8FBB15 2FFE6EE5 50A1972B
D4D7AF1F D298892C D5A2A76B C3462866 13E0E55D DC0C4B92 5AA94B6E 69277F9B
FC73C697 11266E19 451C0FAB A55E6A28 901A48C5 B9911EE6 348A8920 0AED1E10
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 1EDEEB54 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 FFBC8F2D 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
73A1AED 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ポートを保護するための、セキュリティ上のベストプラクティス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ときもパケット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、[コントロールプレーン ポリシング](#)のマニュアル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
```

Cisco SRST でのセキュアな SIP コール シグナリングおよび SRTP メディアの設定

Cisco Unified Survivable Remote Site Telephony (Cisco SRST) は、セキュアなコール シグナリングと、メディア暗号化のための Secure Real-Time Transport Protocol (SRTP) を提供します。これにより、Cisco Unified IP Phone とゲートウェイ デバイスの間でセキュアな暗号化された接続を確立できます。

- [Cisco SRST でセキュアな SIP コール シグナリングおよび SRTP メディアを設定するための前提条件 \(209 ページ\)](#)
- [Cisco SRST でのセキュアな SIP コール シグナリングおよび SRTP メディアの設定に関する制約事項 \(209 ページ\)](#)
- [Cisco Unified SIP SRST のセキュア SIP シグナリングおよび SRTP メディアのサポートについて \(210 ページ\)](#)
- [Cisco Unified Communications Manager の設定 \(210 ページ\)](#)
- [電話の設定 \(211 ページ\)](#)
- [セキュア SIP SRST の SIP オプションの設定 \(212 ページ\)](#)
- [SIP SRST セキュリティ ポリシーの設定 \(213 ページ\) \(任意\)](#)
- [セキュア SIP SRST の SIP ユーザ エージェントの設定 \(214 ページ\) \(任意\)](#)
- [設定の確認 \(216 ページ\)](#)
- [Cisco Unified SIP SRST の設定例 \(217 ページ\)](#)

Cisco SRST でセキュアな SIP コール シグナリングおよび SRTP メディアを設定するための前提条件

- Cisco IOS リリース 15.0(1)XA 以降。
- Cisco Unified IP Phone ファームウェア リリース 8.5(3) 以降。
- 「バックツーバック ユーザ エージェント モードを使用する SIP SRST 機能を設定するための前提条件」に記載された前提条件と必須作業の完了。
- 「セキュア通信のための Cisco Unified SRST ルータの準備」に記載された、証明書を使用するための Cisco Unified SIP SRST デバイスの準備。

Cisco SRST でのセキュアな SIP コール シグナリングおよび SRTP メディアの設定に関する制約事項

SIP 電話は Cisco Unified CM で認証済みデバイス セキュリティ モードに設定できます。Cisco Unified CM は、シグナリングに NULL-SHA 暗号を使用する TLS 接続によって、電話機の整合性と認証を保証します。認証済みの SIP 電話が Cisco Unified SRST デバイスにフェールオーバーする場合は、デバイスが TLS/TCP ではなく TCP を使用して登録されるため、SIP 電話が Cisco Unified CM にフェールバックするまで認証済みモードは無効になります。

- デフォルトでは、非セキュア TCP SIP 電話は、プライマリ コール制御からのフェールオーバー時に SRST デバイスへの登録が許可されます。TCP SIP 電話のサポートには、暗号化された電話機が導入されていない場合でも、ここで説明するセキュア SRST の設定が必要です。セキュア SIP SRST が設定されていない場合、TCP 電話は、シグナリング転送用の UDP を使用して SRST デバイスに登録されます。

Cisco Unified SIP SRST のセキュア SIP シグナリングおよび SRTP メディアのサポートについて

Cisco IP Phone ファームウェア 8.5(3) および Cisco IOS リリース 15.0(1)XA 以降、Cisco SRST は、RTP と SRTP の両方のメディア接続が IP 電話のセキュリティ設定に基づいている場合に、UDP、TCP、および TLS 接続を介した SIP シグナリングをサポートします。

Cisco SRST の SIP-to-SIP および SIP-to-PSTN サポートには、次の機能が含まれます。

- 基本的なコール
- 保留/復帰
- 会議
- 転送
- ブラインド転送
- コール転送

Cisco SRST の SIP-to-Other (SIP-to-SCCP を含む) サポートには基本的なコールが含まれます(ただし、他の機能が動作することがあります)。

Cisco Unified Communications Manager の設定

SCCP で制御されるデバイスと同様に、SIP で制御されるデバイスは、割り当てられたデバイスプールにリストされる SRST リファレンス プロファイルを使用します。WAN に障害が発生した場合に SIP/TLS 通信が必要な場合は、SRST リファレンス プロファイルで [SRST はセキュアか (Is SRST Secure)] チェックボックスがオンになっている必要があります。



(注)

すべての Cisco Unified IP Phone のファームウェアがバージョン 8.5(3) 以降に更新されている必要があります。8.5(3) より前のファームウェアを持つデバイスには、[SRST はセキュアか (Is SRST Secure)] オプションがオフの状態で作成された別のデバイスプールおよび SRST リファレンス プロファイルが必要です。このデバイスプールの SIP で制御されたデバイスは、UDP を介して SIP を使用して SRST ルータへの登録を試みます。

Cisco Unified CM Administration で、[システム (System)] > [SRST] を選択し、次のことを確認します。

- セキュアな SRST プロファイルの場合は、[SRST はセキュアか (Is SRST Secure?)] をオンにする必要があります。SIP ポートは 5061 である必要があります。
- セキュアでない SRST プロファイルの場合は、[SRST はセキュアか (Is SRST Secure?)] チェックボックスをオンにしないでください。また、SIP ポートは 5060 である必要があります。

[デバイス (Device)] > [電話 (Phone)] を選択し、次のことを確認します。

- セキュアな電話機はセキュアな SRST プロファイルを使用するプールに属する必要があります。
- セキュアでない電話機はセキュアでない SRST プロファイルを使用するプールに属する必要があります。



(注) SIP 電話は、電話セキュリティ プロファイルによってそれらに割り当てられた転送方式を使用します。

電話の設定

ここでは、SRTP を使用してセキュアなコールを有効にする必要があることを指定し、セキュアでないコールが RTP メディアを使用して「フォールバック」することを許可します。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **srtp**
5. **allow-connections sip to h323**
6. **allow-connections sip to sip**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
手順 1	enable 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	configure terminal 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	voice service voip 例: Router(config)# voice service voip	音声サービス コンフィギュレーション モードを開始します。
手順 4	srtp 例: Router(config-voi-serv)# srtp	SRTP を使用してセキュアなコールを有効にするように指定します。

■ セキュアな Unified SRST の設定方法

	コマンドまたはアクション	目的
手順 5	<code>allow-connections sip to h323</code> 例: Router(config-voi-serv)# allow-connections sip to h323	(任意)SIP エンドポイントから H.323 エンドポイントへの接続を許可します。
手順 6	<code>allow-connections sip to sip</code> 例: Router(config-voi-serv)# allow-connections sip to sip	SIP エンドポイントから SIP エンドポイントへの接続を許可します。
手順 7	<code>end</code> 例: Router(conf-voi-serv)# end	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。

セキュア SIP SRST の SIP オプションの設定

ここでは、セキュア SIP SRTP を設定する方法について説明します。

手順の概要

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `sip`
5. `url sip | sips`
6. `srtp negotiate cisco`
7. `end`

手順の詳細

	コマンドまたはアクション	目的
手順 1	<code>enable</code> 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
手順 2	<code>configure terminal</code> 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
手順 3	<code>voice service voip</code> 例: Router(config)# voice service voip	音声サービス 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
手順 4	<code>sip</code> 例: Router(config-voi-serv)# sip	SIP コンフィギュレーション モードを開始します。
手順 5	<code>url sip sips</code> 例: Router(conf-serv-sip)# url sips	セキュア モードを設定するには、 sips キーワードを使用して URL を VoIP コールの SIP Secure (SIPS) 形式で生成します。 デバイスデフォルト モードを設定するには、 sip キーワードを使用して URL を VoIP コールの SIP 形式で生成します。
手順 6	<code>srtplib negotiate cisco</code> 例: Router(conf-serv-sip)# srtplib negotiate cisco	SRTP オファラーの応答時に Cisco IOS SIP ゲートウェイが RTP プロファイルの送信と受信をネゴシエートできるようにします。
手順 7	<code>end</code> 例: Router(conf-serv-sip)# end	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。

SIP SRST セキュリティ ポリシーの設定

ここでは、セキュア モードで、セキュアでない電話機の SRST ルータへの登録をブロックする方法について説明します。

手順の概要

1. `voice register global`
2. `security-policy secure | no security-policy`
3. `end`

手順の詳細

	コマンドまたはアクション	目的
手順 1	<code>voice register global</code> 例: Router(config)# voice register global	音声レジスタ グローバル コンフィギュレーション モードを開始します。
手順 2	<code>security-policy secure</code> 例: Router(config-register-global)# security-policy secure	SIP/TLS/TCP 接続だけが許可されるよう SIP 登録セキュリティ ポリシーを設定します。デバイスデフォルトモードの場合は、 no security-policy コマンドを使用します。デバイスデフォルトモードでは、セキュアでないデバイスの TLS を使用しない登録が許可されます。 (注) security-policy secure をセキュア SRST 機能に対して設定し、非セキュア電話機がセキュア SRST にフォールバックしないようにすることを推奨します。
手順 3	<code>end</code> 例: Router(config-register-global)# end	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。

セキュア SIP SRST の SIP ユーザ エージェントの設定

ここでは、厳密な暗号によって、許可される暗号化アルゴリズムを制限する方法について説明します。

手順の概要

1. `sip-ua`
2. `registrar ipv4:destination-address expires seconds`
3. `xfer target dial-peer`
4. `crypto signaling default trustpoint string [strict-cipher]`
5. `crypto signaling remote-addr {ip address [subnet mask]} trustpoint trustpoint-name`
6. `end`

手順の詳細

	コマンドまたはアクション	目的
手順 1	<code>sip-ua</code> 例: Router(config)# sip-ua	SIP ユーザ エージェント コンフィギュレーション モードを開始します。
手順 2	<code>registrar ipv4:destination-address expires seconds</code> 例: Router(config-sip-ua)# registrar ipv4:192.168.2.10 expires 3600	ゲートウェイがプライマリおよびセカンダリ外部 SIP レジストラに E.164 電話番号を登録できるようにします。 <code>destination-address</code> はプライマリ SIP レジストラ サーバの IP アドレスです。

	コマンドまたはアクション	目的
手順 3	xfer target dial-peer 例: Router(config-sip-ua)# xfer target dial-peer	SRST が転送先として、メッセージ本文で指定されたものではなくダイヤル ピアを使用するよう指定します。
手順 4	crypto signaling default trustpoint string [strict-cipher] 例: Router(config-sip-ua)# crypto signaling default trustpoint 3745-SRST strict-cipher	TLS ハンドシェイク中に使用される trustpoint string キーワードおよび引数を識別します。 trustpoint string キーワードおよび引数は、Cisco IOS Public Key Infrastructure (PKI) コマンドを使用して、登録プロセスの一部として生成されたゲートウェイの証明書を参照します。 strict-cipher キーワードは、Advanced Encryption Standard-128 (AES-128) Cipher-Block-Chaining (CBC) セキュア ハッシュ アルゴリズム (SHA) (TLS_RSA_WITH_AES_128_CBC_SHA) 暗号スイートでの TLS RSA 暗号化のサポートを制限します。 デバイスデフォルト モードを設定するには、 strict-cipher キーワードを省略します。
手順 5	crypto signaling remote-addr {ip address /subnet mask} trustpoint trustpoint-name 例: Router(config-sip-ua)# crypto signaling remote-addr 8.41.20.20 255.255.0.0 trustpoint srst-trunk1	トラストポイント ラベルは、登録プロセスの一部として Cisco IOS PKI コマンドで生成される CUBE の証明書を指します。 キーワードと引数は次のとおりです。 <ul style="list-style-type: none"> • remote-addr ip address: トラストポイントに IP アドレスを関連付けます。 • trustpoint trustpoint-name: Cisco IOS PKI コマンドを使用した登録プロセスの一環として生成された SIP ゲートウェイ証明書を指します。
手順 6	end 例: Router(config-sip-ua)# end	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。

複数のトラストポイント

セキュア モードで Unified SRST に登録する電話機に対しては、**sip-ua** 設定モードの下でデフォルトのトラストポイント設定を使用します。たとえば、**srstca** は、セキュア SRST のデフォルトのトラストポイントです。このデフォルトのシグナリング トラストポイントは、SIP 電話から Unified セキュア SRST ルータへのすべての SIP TLS 相互作用に使用されます。

複数のトラストポイントがある導入シナリオでは、CA 発行の証明書でのセキュア トランクを介したサービスプロバイダーとの通信は、**sip-ua** 設定モードの下で、CLI コマンド **crypto signaling remote-addr 8.41.20.20 255.255.0.0 trustpoint srst-trunk1** を使用して実現されます。

例

次に示すのは、Unified SRST 導入の複数のトラストポイントの設定例です。この例では、**srst-trunk1** トラストポイントは IP アドレス **8.39.0.0** のネットワークを指示し、**srst-trunk2** トラストポイントは IP アドレス **8.41.20.20** のネットワークを指示します。

```
sip-ua
crypto signaling remote-addr 8.39.0.0 255.255.0.0 trustpoint srst-trunk1
crypto signaling remote-addr 8.41.20.20 255.255.0.0 trustpoint srst-trunk2
crypto signaling default trustpoint secrst
```

設定の確認

次の例は、**show sip-ua status registrar** コマンドと **show voice register global** コマンドによって表示された設定例を示しています。

特権 EXEC モードで **show sip-ua status registrar** コマンドを使用すると、連絡先アドレスに現在登録されているすべての SIP エンドポイントが表示されます。

```
Router# show sip-ua status registrar
Line          destination      expires(sec)  contact
transport    call-id
              peer
=====
3029991      192.168.2.108   388           192.168.2.108
TLS          00120014-4ae40064-f1a3e9fe-8d301072@192.168.2.1
40004
3029993      192.168.2.103   382           192.168.2.103
TCP          001bd433-1c840052-655cd596-4e992eed@192.168.2.1
40011
3029982      192.168.2.106   406           192.168.2.106
UDP          001d452c-dbba0056-0481d321-1f3f848d@192.168.2.1
40001
3029983      192.168.2.106   406           192.168.2.106
UDP          001d452c-dbba0057-1c69b699-d8dc6625@192.168.2.1
40003
3029992      192.168.2.107   414           192.168.2.107
TLS          001e7a25-50c9002c-48ef7663-50c71794@192.168.2.1
40005
```

特権 EXEC モードで **show voice register global** コマンドを使用すると、SIP 電話に関連付けられたすべてのグローバル コンフィギュレーション パラメータが表示されます。

```
Router# show voice register global
CONFIG [Version=8.0]
=====
Version 8.0
Mode is srst
Max-pool is 50
Max-dn is 100
Outbound-proxy is enabled and will use global configured value
Security Policy: DEVICE-DEFAULT
timeout interdigit 10
network-locale[0] US (This is the default network locale for this box)
network-locale[1] US
network-locale[2] US
network-locale[3] US
network-locale[4] US
user-locale[0] US (This is the default user locale for this box)
user-locale[1] US
user-locale[2] US
user-locale[3] US
user-locale[4] US
Router#
```

Cisco Unified SIP SRST の設定例

```
Current configuration : 15343 bytes
!
! Last configuration change at 05:34:06 UTC Tue Jun 13 2017
! NVRAM config last updated at 11:57:03 UTC Thu Jun 8 2017
!
version 16.7
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname router
!
boot-start-marker
boot-end-marker
!

vrf definition Mgmt-intf
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
!
! card type command needed for slot/bay 0/3
no logging queue-limit
logging buffered 20000000
no logging rate-limit
no logging console
enable password xxxx
!
no aaa new-model
!
subscriber templating
!
multilink bundle-name authenticated
!
crypto pki server SRST-CA-2
 database level complete
 no database archive
 grant auto
!
crypto pki trustpoint TRUSTPT-SRST-CA-2
 enrollment url http://10.0.0.1:80
 serial-number
 revocation-check none
 rsakeypair srstcakey 2048
 rsakeypair SRST-CA-2
!
crypto pki trustpoint SRST-CA-2
 revocation-check crl
 rsakeypair SRST-CA-2
!
crypto pki trustpoint Cisco_Manufacturing_CA
 enrollment terminal
 revocation-check none
!
crypto pki trustpoint CAPF-3a66269a
 enrollment terminal
 revocation-check none
```

```

!
crypto pki trustpoint Cisco_Root_CA_2048
  enrollment terminal
  revocation-check none
!
!
crypto pki certificate chain TRUSTPT-SRST-CA-2
certificate 02
 3082020B 30820174 A0030201 02020102 300D0609 2A864886 F70D0101 05050030
 14311230 10060355 04031309 53525354 2D43412D 32301E17 0D313730 36303831
 31333131 325A170D 31383036 30383131 33313132 5A303231 30301206 03550405
 130B4647 4C313735 31313150 42301A06 092A8648 86F70D01 0902160D 416E7473
 41726D79 2D343430 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030
 81890281 81009E24 6259A98D A61C1973 45A95DA8 DE83ECAD C2B1B448 741F7E64
 3D753BF1 19BD54FB 9A4D4A8E 7A2BA416 B93C40B3 A63A7C4D 7303498F 098EF07F
 96F26F5F 49AD4E39 EC113DF4 696CB887 607D545A 52A11469 958F4C04 05868DF9
 317456F6 3D23837C D46331FA 69FB29E8 3211E01C A7AB19A3 94DAC09F 97601196
 A08D7073 76210203 010001A3 4F304D30 0B060355 1D0F0404 030205A0 301F0603
 551D2304 18301680 142110B8 F25BD9BD E1D401EC 9D11DC0E AE52CDB8 2F301D06
 03551D0E 04160414 2110B8F2 5BD9BDE1 D401EC9D 11DC0EAE 52CDB82F 300D0609
 2A864886 F70D0101 05050003 8181003A DC409694 26D08A31 7B4F495F 002D4E57
 B28669A9 10E93C68 A9556659 97D326EC A5508201 C1A86659 B1CDC910 73097FCA
 F6174794 1057DDDE DBA666D6 0BAFC503 96A10BE5 5FCA3B93 5D377ABE BC9B2774
 3732DF01 CE3BF12B 1899AA69 F7EC8726 A1964C5A D6A99A0E E27EE2A0 15A7D364
 793C6C8D 961C77E4 397F9CB4 C6A271
quit
certificate ca 01
 30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 14311230 10060355 04031309 53525354 2D43412D 32301E17 0D313730 36303831
 31323135 305A170D 32303036 30373131 32313530 5A301431 12301006 03550403
 13095352 53542D43 412D3230 819F300D 06092A86 4886F70D 01010105 0003818D
 00308189 02818100 9E246259 A98DA61C 197345A9 5DA8DE83 ECADC2B1 B448741F
 7E643D75 3BF119BD 54FB9A4D 4A8E7A2B A416B93C 40B3A63A 7C4D7303 498F098E
 F07F96F2 6F5F49AD 4E39EC11 3DF4696C B887607D 545A52A1 1469958F 4C040586
 8DF93174 56F63D23 837CD463 31FA69FB 29E83211 E01CA7AB 19A394DA C09F9760
 1196A08D 70737621 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
 01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 16801421
 10B8F25B D9BDE1D4 01EC9D11 DC0EAE52 CDB82F30 1D060355 1D0E0416 04142110
 B8F25BD9 BDE1D401 EC9D11DC 0EAE52CD B82F300D 06092A86 4886F70D 01010405
 00038181 0018859E D39C6A05 63509442 8746D970 BB716DE2 E82BA822 58AA55AD
 AC37260F 36BFDFE6 F2D0E489 A8D23690 791AD903 F19AC857 5002E621 A5927ACC
 DCB759C0 B126ACAB C53BF054 1F62D895 A895C50A E3AE83E3 EC68F346 50B88D39
 BB053EE9 5D466AE4 C6B4593D 7EFA7A78 213C0766 7307A051 78FED92E 5A34AAB6
 98D2A59C 31
quit
crypto pki certificate chain SRST-CA-2
certificate ca 01
 30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 14311230 10060355 04031309 53525354 2D43412D 32301E17 0D313730 36303831
 31323135 305A170D 32303036 30373131 32313530 5A301431 12301006 03550403
 13095352 53542D43 412D3230 819F300D 06092A86 4886F70D 01010105 0003818D
 00308189 02818100 9E246259 A98DA61C 197345A9 5DA8DE83 ECADC2B1 B448741F
 7E643D75 3BF119BD 54FB9A4D 4A8E7A2B A416B93C 40B3A63A 7C4D7303 498F098E
 F07F96F2 6F5F49AD 4E39EC11 3DF4696C B887607D 545A52A1 1469958F 4C040586
 8DF93174 56F63D23 837CD463 31FA69FB 29E83211 E01CA7AB 19A394DA C09F9760
 1196A08D 70737621 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
 01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 16801421
 10B8F25B D9BDE1D4 01EC9D11 DC0EAE52 CDB82F30 1D060355 1D0E0416 04142110
 B8F25BD9 BDE1D401 EC9D11DC 0EAE52CD B82F300D 06092A86 4886F70D 01010405
 00038181 0018859E D39C6A05 63509442 8746D970 BB716DE2 E82BA822 58AA55AD
 AC37260F 36BFDFE6 F2D0E489 A8D23690 791AD903 F19AC857 5002E621 A5927ACC
 DCB759C0 B126ACAB C53BF054 1F62D895 A895C50A E3AE83E3 EC68F346 50B88D39
 BB053EE9 5D466AE4 C6B4593D 7EFA7A78 213C0766 7307A051 78FED92E 5A34AAB6
 98D2A59C 31

```

```

quit
crypto pki certificate chain Cisco_Manufacturing_CA
certificate ca 6A6967B300000000000003
308204D9 308203C1 A0030201 02020A6A 6967B300 00000000 03300D06 092A8648
86F70D01 01050500 30353116 30140603 55040A13 0D436973 636F2053 79737465
6D73311B 30190603 55040313 12436973 636F2052 6F6F7420 43412032 30343830
1E170D30 35303631 30323231 3630315A 170D3239 30353134 32303235 34325A30
39311630 14060355 040A130D 43697363 6F205379 7374656D 73311F30 1D060355
04031316 43697363 6F204D61 6E756661 63747572 696E6720 43413082 0120300D
06092A86 4886F70D 01010105 00038201 0D003082 01080282 010100A0 C5F7DC96
943515F1 F4994EBB 9B41E17D DB791691 BBF354F2 414A9432 6262C923 F79AE7BB
9B79E807 294E30F5 AE1BC521 5646B0F8 F4E68E81 B816CCA8 9B85D242 81DB7CCB
94A91161 121C5CEA 33201C9A 16A77DD8 99066AE2 36AFECF8 0AFF9867 07F430EE
A5F8881A AAE8C73C 1CCEEE48 FDCD5C37 F186939E 3D71757D 34EE4B14 A9C0297B
0510EF87 9E693130 F548363F D8ABCE15 E2E8589F 3E627104 8726A415 620125AA
D5DFC9C9 5BB8C9A1 077BBE68 92939320 A86CBD15 75D3445D 454BECA8 DA60C7D8
C8D5C8ED 41E1F55F 578E5332 9349D5D9 0FF836AA 07C43241 C5A7AF1D 19FFF673
99395A73 67621334 0D1F5E95 70526417 06EC535C 5CDB6AEA 35004102 0103A382
01E73082 01E33012 0603551D 130101FF 04083006 0101FF02 0100301D 0603551D
0E041604 14D0C522 26AB4F46 60ECAE05 91C7DC5A D1B047F7 6C300B06 03551D0F
04040302 01863010 06092B06 01040182 37150104 03020100 30190609 2B060104
01823714 02040C1E 0A005300 75006200 43004130 1F060355 1D230418 30168014
27F3C815 1E6E9A02 0916AD2B A089605F DA7B2FAA 30430603 551D1F04 3C303A30
38A036A0 34863268 7474703A 2F2F7777 772E6369 73636F2E 636F6D2F 73656375
72697479 2F706B69 2F63726C 2F637263 61323034 382E6372 6C305006 082B0601
05050701 01044430 42304006 082B0601 05050730 02863468 7474703A 2F2F7777
772E6369 73636F2E 636F6D2F 73656375 72697479 2F706B69 2F636572 74732F63
72636132 3034382E 63657230 5C060355 1D200455 30533051 060A2B06 01040109
15010200 30433041 06082B06 01050507 02011635 68747470 3A2F2F77 77772E63
6973636F 2E636F6D 2F736563 75726974 792F706B 692F706F 6C696369 65732F69
6E646578 2E68746D 6C305E06 03551D25 04573055 06082B06 01050507 03010608
2B060105 05070302 06082B06 01050507 03050608 2B060105 05070306 06082B06
01050507 0307060A 2B060104 0182370A 0301060A 2B060104 01823714 02010609
2B060104 01823715 06300D06 092A8648 86F70D01 01050500 03820101 0030F330
2D8CF2CA 374A6499 24290AF2 86AA42D5 23E8A2EA 2B6F6923 7A828E1C 4C09CFA4
4FAB842F 37E96560 D19AC6D8 F30BF5DE D027005C 6F1D91BD D14E5851 1DC9E3F7
38E7D30B D168BE8E 22A54B06 E1E6A4AA 337D1A75 BA26F370 C66100A5 C379265B
A719D193 8DAB9B10 11291FA1 82FDFD3C 4B6E65DC 934505E9 AF336B67 23070686
22DAEBDC 87CF5921 421AE9CF 707588E0 243D5D7D 4E963880 97D56FF0 9B71D8BA
6019A5B0 6186ADDD 6566F6B9 27A2EE2F 619BBAA1 3061FDBE AC3514F9 B82D9706
AFC3EF6D CC3D3CEB 95E981D3 8A5EB6CE FA79A46B D7A25764 C43F4CC9 DBE882EC
0166D410 88A256E5 3C57EDE9 02A84891 6307AB61 264B1A13 9FE4DCDA 5F
quit
crypto pki certificate chain CAPF-3a66269a
certificate ca 583BD5B4844C8BC172B8C4979092A067
308203C3 308202AB A0030201 02021058 3BD5B484 4C8BC172 B8C49790 92A06730
0D06092A 864886F7 0D01010B 05003071 310B3009 06035504 06130249 4E310E30
0C060355 040A0C05 63697363 6F311230 10060355 040B0C09 75637467 2D656467
65311630 14060355 04030C0D 43415046 2D336136 36323639 61311230 10060355
04080C09 6B61726E 6174616B 61311230 10060355 04070C09 62616E67 616C6F72
65301E17 0D313730 35323931 30333631 335A170D 32323035 32383130 33363132
5A307131 0B300906 03550406 1302494E 310E300C 06035504 0A0C0563 6973636F
31123010 06035504 0B0C0975 6374672D 65646765 31163014 06035504 030C0D43
4150462D 33613636 32363961 31123010 06035504 080C096B 61726E61 74616B61
31123010 06035504 070C0962 616E6761 6C6F7265 30820122 300D0609 2A864886
F70D0101 01050003 82010F00 3082010A 02820101 00BC774F BAED3986 05BDFBFC
4EABBF7A 1F73D150 2989EFF2 902502F6 248DA7AB 261E474C 08A4BB6F 35B10449
0A6A3D94 E2C6EB98 57BECE0C 34F30517 CA6CC9B2 710B511B 8826E0AB 733FF26F
F7ADC4B9 76118300 6156072C 43F78E5E 3AD7C92B 54CB5BDB 00B53FC8 875100C4
056BC4A7 0F96CE69 E58B1C22 194CCEC6 968ECF9B 08B7B7B2 0FF0800E 43764BB1
E6ED36C0 A738F762 81A88F6D E464E2A5 FD74207F 1EC7ACAC 2F63B04D E0E9DA4C
901A1710 E3D1C069 82EFF77E 0597254D 149C1263 EC67DAE9 305FD8BF C7410B17
8C6DE9FF 28A37514 86AF828C BC698DD5 F18A3B66 9D8D895A 5562E08D 383F790A
A5C7F6F6 915CB558 042E5B99 71F7169D B3AFA699 2B020301 0001A357 3055300B

```

```

0603551D 0F040403 0202A430 13060355 1D25040C 300A0608 2B060105 05070301
301D0603 551D0E04 16041475 71EC5D35 1A431511 7E8C8462 6E65E570 7C551930
12060355 1D130101 FF040830 060101FF 02010030 0D06092A 864886F7 0D01010B
05000382 0101008F 0D3E9F3E 3574100D 97AD876D B4015C21 300A1BD0 59D5C9BF
41A8448D 597CD278 718A6431 BA94C042 7EC64BA0 71F04501 C33C1664 16484373
F3C226A7 256363A9 8BE97291 6B25B8B4 E3DB84C3 3DDB63E7 A9D8D577 6B8F37B3
7CFCE019 D6F09573 946191F7 C4028465 B072DF74 9D6DED45 CA9E6A3B 1401D1A3
5449EDCE 9FA593E3 2FD71031 C7C7EB9C 045DAAFE C67603BF DAB40EE0 352C009F
EAAA6816 A11F6D8B 7C406211 1045A0C6 488B34E1 AF968FAF 3705A364 1EE21A1D
B7080EDC 40D4AA15 E110C5F1 D8A57561 DB2B09F1 0779B855 3998CE22 C471B5CB
09605E24 99855176 2D1CA40E BEBC2F23 7434CA2B 8D1C5EFB 822147CC 81F98825
47A1A14F DC5480
quit
crypto pki certificate chain Cisco_Root_CA_2048
certificate ca 5FF87B282B54DC8D42A315B568C9ADFF
30820343 3082022B A0030201 0202105F F87B282B 54DC8D42 A315B568 C9ADFF30
0D06092A 864886F7 0D010105 05003035 31163014 06035504 0A130D43 6973636F
20537973 74656D73 311B3019 06035504 03131243 6973636F 20526F6F 74204341
20323034 38301E17 0D303430 35313432 30313731 325A170D 32393035 31343230
32353432 5A303531 16301406 0355040A 130D4369 73636F20 53797374 656D7331
1B301906 03550403 13124369 73636F20 526F6F74 20434120 32303438 30820120
300D0609 2A864886 F70D0101 01050003 82010D00 30820108 02820101 00B09AB9
ABA7AF0A 77A7E271 B6B46662 94788847 C6625584 4032BFC0 AB2EA51C 71D6BC6E
7BA8AABA 6ED21588 48459DA2 FC83D0CC B98CE026 68704A78 DF21179E F46105C9
15C8CF16 DA356189 9443A884 A8319878 9BB94E6F 2C53126C CD1DAD2B 24BB31C4
2BFF8344 6FB63D24 7709EABF 2AA81F6A 56F6200F 11549781 75A725CE 596A8265
EFB7EAE7 E28D758B 6EF2DD4F A65E629C CF100A64 D04E6DCE 2BCC5BF5 60A52747
8D69F47F CE1B70DE 701B20D6 6ECDA601 A83C12D2 A93FA06B 5EBB8E20 8B7A91E3
B568EEA0 E7C40174 A8530B2B 4A9A0F65 120E824D 8E63FDEF EB9B1ADB 53A61360
AFC27DD7 C76C1725 D473FB47 64508180 944CE1BF AE4B1CDF 92ED2E05 DF020103
A351304F 300B0603 551D0F04 04030201 86300F06 03551D13 0101FF04 05300301
01FF301D 0603551D 0E041604 1427F3C8 151E6E9A 020916AD 2BA08960 5FDA7B2F
AA301006 092B0601 04018237 15010403 02010030 0D06092A 864886F7 0D010105
05000382 0101009D 9D8484A3 41A97C77 0CB753CA 4E445062 EF547CD3 75171CE8
E0C6484B B6FE4C3A 198156B0 56EE1996 62AA5AA3 64C1F64E 5433C677 FEC51CBA
E55D25CA F5F0939A 83112EE6 CBF87445 FEE705B8 ABE7DFCB 4BE13784 DAB98B97
701EF0E2 8BD7B0D8 0E9DB169 D62A917B A9494F7E E68E95D8 83273CD5 68490ED4
9DF62EEB A7BEEB30 A4AC1F44 FC95AB33 06FB7D60 0ADEB48A 63B09CA9 F2A4B953
0187D068 A4277FAB FFE9FAC9 40388867 B439C684 6F57C953 DBBA8EEE C043B2F8
09836EFF 66CF3EEF 17B35818 2509345E E3CBD614 B6ECF292 6F74E42F 812AD592
91E0E097 3C326805 854BD1F7 57E2521D 931A549F 0570C04A 71601E43 0B601EFE
A3CE8119 E10B35
quit
!
voice service voip
no ip address trusted authenticate
media bulk-stats
media disable-detailed-stats
allow-connections sip to sip
srtp
no supplementary-service sip refer
supplementary-service media-renegotiate
no supplementary-service sip handle-replaces
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
sip
registrar server expires max 120 min 60
!
voice register global
default mode
no allow-hash-in-dn
security-policy secure
max-dn 50
max-pool 40
!

```



```
voice register pool 1
  id network 10.0.0.1 mask 255.255.0.0
  dtmf-relay rtp-nte
  codec g711ulaw
!
voice hunt-group 1 sequential
  final 89898
  list 1008,2005
  timeout 5
  pilot 1111
!
voice-card 0/1
  no watchdog
!
voice-card 0/2
  no watchdog
!
voice-card 0/3
  no watchdog
!
voice-card 1/0
  no watchdog
!
license udi pid ISR4451-X/K9 sn FOC1743565L
license accept end user agreement
license boot level uck9
license boot level securityk9
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
redundancy
  mode none
!
interface GigabitEthernet0/0/0
  ip address 10.0.0.1 255.255.0.0
  negotiation auto
!
interface GigabitEthernet0/0/1
  no ip address
  negotiation auto
!
interface GigabitEthernet0/0/2
  ip address 10.0.0.1 255.0.0.0
  negotiation auto
!
interface GigabitEthernet0/0/3
  no ip address
  negotiation auto
!
interface Service-Engine0/1/0
  shutdown
!
interface Service-Engine0/2/0
  shutdown
!
interface Service-Engine0/3/0
!
interface Service-Engine1/0/0
!
interface GigabitEthernet0
  vrf forwarding Mgmt-intf
  no ip address
  negotiation auto
```

```

!
ip forward-protocol nd
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.0.0.1
!
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
control-plane
!
!
voice-port 0/1/0
!
voice-port 0/1/1
!
voice-port 0/2/0
!
voice-port 0/2/1
!
voice-port 0/2/2
!
voice-port 0/2/3
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
sip-ua
  crypto signaling default trustpoint TRUSTPT-SRST-CA-2
!
!
credentials
  ip source-address 10.0.0.1 port 2445
  trustpoint TRUSTPT-SRST-CA-2
!
!
call-manager-fallback
max-conferences 8 gain -6
transfer-system full-consult
max-ephones 50
max-dn 50
call-park system application
fac standard
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
stopbits 1
line aux 0
stopbits 1
line vty 0 4
exec-timeout 0 0
password xxxx
no login
length 0
transport preferred none
transport input telnet ssh
!
end

```

その他の関連資料

ここでは、この機能に関連する参照資料を提供します。

関連資料

関連項目	参照先
Cisco IOS の音声設定	<ul style="list-style-type: none"> 『Cisco IOS Voice Configuration Library』 『Cisco IOS Voice Command Reference』
『Cisco Unified Communications Manager Documentation Guide for Release 8.0(2)』	<ul style="list-style-type: none"> 『Cisco Unified Communications Manager Documentation Guide for Release 8.0(2)』
Cisco Unified SRST の設定	<ul style="list-style-type: none"> 『Cisco Unified SRST and SIP SRST Command Reference』
Cisco Unified SRST	<ul style="list-style-type: none"> 『Cisco Unified SRST 8.0 Supported Firmware, Platforms, Memory, and Voice Products』
『Cisco Unified Communications Operating System Administration Guide, Release 6.1(1)』	<ul style="list-style-type: none"> セキュリティ
セキュア Survivable Remote Site Telephony (SRST) リファレンスの設定	<ul style="list-style-type: none"> 「Configuring a Secure Survivable Remote Site Telephony (SRST) Reference」

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	<p>選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p>http://www.cisco.com/go/mibs</p>

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

テクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ただけのように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報入手するために、Product Alert Tool (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/techsupport</p>

コマンドリファレンス

次のコマンドは、このセクションで説明した機能で導入または修正されたものです。これらのコマンドについては、『Cisco IOS Voice Command Reference』(http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html)を参照してください。すべての Cisco IOS コマンドについては、<http://tools.cisco.com/Support/CLILookup> でコマンド検索ツールを使用するか、http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html で『Cisco IOS Master Command List, All Releases』を参照してください。

- **security-policy**
- **show voice register global**
- **show voice register all**

セキュア SCCP および SIP SRST の機能情報

表 8-4 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンドリファレンスマニュアルを参照してください。

プラットフォームのサポート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検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、Cisco IOS および Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャセット、またはプラットフォームを確認できます。Cisco Feature Navigator にアクセスするには、<http://www.cisco.com/go/cfn> に移動します。Cisco.com のアカウントは必要ありません。



(注) 表 8-4 に、特定の Cisco IOS ソフトウェア リリース トレインの中で特定の機能のサポートが導入された Cisco IOS ソフトウェア リリースだけを示します。その機能は、特に断りがない限り、それ以降の一連の Cisco IOS ソフトウェア リリースでもサポートされます。

表 8-4 Cisco SRST でのセキュア SIP コール シグナリングおよび SRTP メディアの機能情報

機能名	リリース	機能情報
Cisco SRST でのセキュア SIP コール シグナリングおよび SRTP メディア	15.0(1)XA	セキュアなコール シグナリングに対する Session Initiation Protocol/Transport Layer Security/Transmission Control Protocol (SIP/TLS/TCP) サポートとメディア暗号化に対する Secure Real-time Transport Protocol (SRTP) のサポートが追加され、Cisco Unified Survivable Remote Site Telephony (Cisco SRST) を使用して Cisco Unified IP Phone とフェールオーバー デバイス間でセキュアな暗号化された接続を確立できます。次のコマンドが導入または変更されました。 security-policy 、 show voice register global 、 show voice register all 。

次の作業

ボイスメールが必要な場合は、「[ボイスメールと Cisco Unified SRST の統合](#)」セクション (243 ページ) のボイスメールの設定手順を参照してください。

詳細については、「[Cisco Unified SRST 機能の概要](#)」セクション (1 ページ) の章の「[その他の関連資料](#)」セクション (28 ページ) を参照してください。

■ 次の作業



Unified SRST での SIP トランキングの設定

この章では、Cisco Unified Survivable Remote Site Telephony (Unified SRST) の SIP トランキングを設定する方法について説明します。

目次

この章では、Unified SRST でのさまざまな回線側と SIP トランキング機能に関する設定の推奨と詳細について説明します。また、Unified Border Element と Unified SRST のコロケーションについても説明しています。

- [Unified SRST と Unified Border Element のコロケーション \(227 ページ\)](#)
- [Unified SRST と Unified Border Element のコロケーションの設定推奨 \(229 ページ\)](#)

Unified SRST と Unified Border Element のコロケーション

Unified SRST リリース 12.1 以降のリリースでは、Cisco Unified Border Element と Unified SRST (SIP 専用) 製品インスタンスを、同じ Cisco 4000 シリーズ サービス統合型ルータ上に展開できません。Unified SRST と Unified Border Element のコロケーションは、Cisco IOS XE Fuji 16.7.1 リリースでサポートされます。Cisco IP Phone 7800 シリーズおよび Cisco IP Phone 8800 シリーズはこの導入でサポートされます。

ワイドエリア ネットワーク (WAN) が使用可能であると、ルータは、Unified SRST としてではなく、純粋な Cisco Unified Border Element として機能します。

WAN の停止時に、Unified Communications Manager に登録されている電話は、Unified SRST にフォールバックします。ただし、Unified SRST に登録されている電話は、SIP トランクを介して PSTN コールを発信または受信できます。

Unified SRST と Unified Border Element の機能セットは、前述の機能に制限されます。次の機能は、Unified SRST に登録されたときの電話でサポートされます。

- 着信または発信の基本的なコール
- 保留/復帰
- コール転送 (コール受信時に転送)
- コール転送 (コール受信後に転送)
- 会議 (組み込みブリッジ)

- ・ ハント グループ

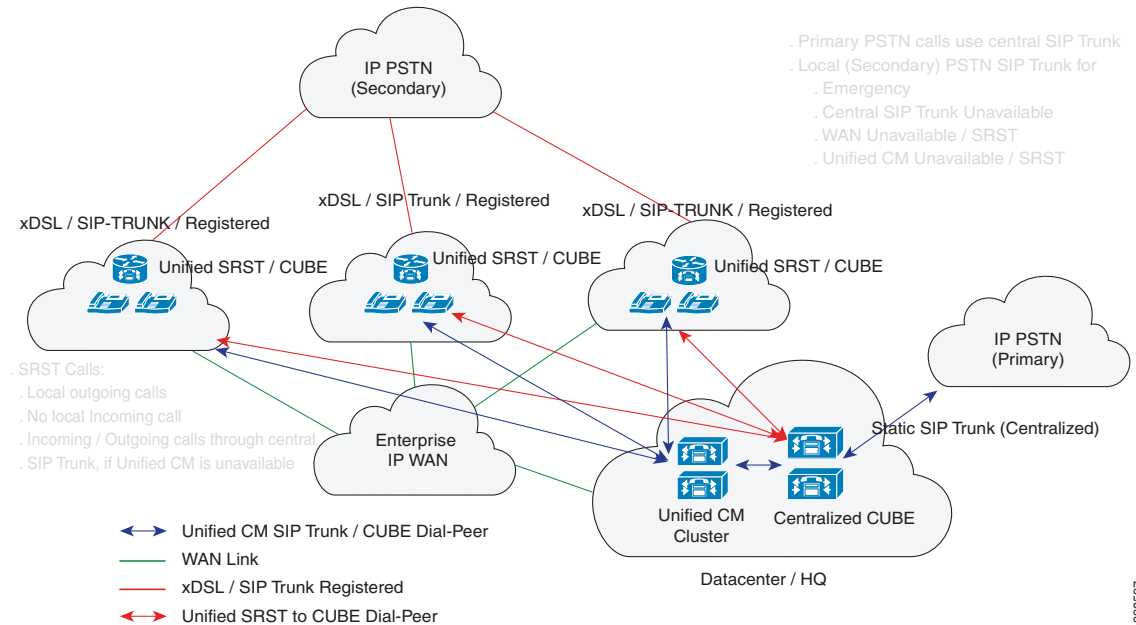
Unified SRST と Unified Border Element のコロケーションでサポートされている SIP トランク機能の一覧は次のとおりです。

- ・ SIP UA 登録/認証、登録、登録/登録更新
- ・ SIP-Server、発信プロキシ
- ・ DNS サービス レコード
- ・ バインド グローバル/ダイヤルピア
- ・ SRTP/TLS、SRTP-RTP インターワーキング
- ・ 接続の再使用
- ・ IP 信頼リスト
- ・ 音声クラス テナント
- ・ RTP-NTE DTMF
- ・ P-Called-Party ID、プライバシー ヘッダー (PAI)
- ・ SIP の正規化

SIP トランクのテナントを設定する方法の詳細については、『[Cisco Unified Border Element Configuration Guide](#)』を参照してください。Unified Border Element のコロケーションに対する推奨設定の詳細については、[Unified SRST と Unified Border Element のコロケーションの設定推奨 \(229 ページ\)](#)を参照してください。

図 9-1 は、Cisco Unified Border Element と Unified SRST のコロケーション導入を示します。

図 9-1 Unified SRST と Cisco Unified Border Element のコロケーション導入



3905697

Unified SRST と Unified Border Element のコロケーションの設定推奨

電話 (Unified Communications Manager に登録済み) が Unified SRST 上でフォールバックした後、作成されるダイヤルピアは、ダイナミックダイヤルピアです。したがって、**voice service voip** および **sip-ua** の下での設定は、それらのダイナミックダイヤルピアから継承されます。**voice service voip** および **sip-ua** の設定を **voice class tenant** 設定モードの下に移動させて、設定の競合を回避します。**voice class tenant** は、SIP トランクダイヤルピア設定に含まれています。

同様に、関連するグローバル設定は **voice class tenant** の下でグループ化され、Unified Communications Manager へのダイヤルピアにも適用できます。**voice class tenant** の下にグループ化されているこれらの設定は、Unified Communications Manager が使用可能である (WAN が使用可能である) ときはいつでも使用されます。Unified SRST と Unified Border Element のコロケーション導入の構成例については、例 (231 ページ) を参照してください。

Unified SRST と Unified Border Element のコロケーションの構成推奨を次に示します。

- SIP トランク固有の **voice service voip** と **sip-ua** の設定を **voice class tenant** の下に移動させます。これは SIP トランクと回線側ダイヤルピアの設定で競合を避けるためです。テナントをダイヤルピアの下で設定すると、設定は次の優先順位で適用されます。
 - ダイヤルピア コンフィギュレーション
 - テナント設定
 - グローバル設定



(注) **tenant** の下に移動させる必要がある特定の CLI コマンドは、**dial-peer** 設定モードの下に移動させます。これは、それらの CLI が **voice class tenant** の下では使用できないからです。たとえば、CLI コマンド **srtplib fallback** は、**voice class tenant** ではなく **dial-peer** 設定モードの下で設定する必要があります。

- ダイヤルピアグループ機能を使用して、複数の発信ダイヤルピアを1つのダイヤルピアグループにまとめ、そのダイヤルピアグループを受信ダイヤルピア (Unified CM トランク) の宛先として設定します。ダイヤルピアグループの詳細については、『[Dial Peer Configuration Guide](#)』を参照してください。
- Unified Communications Manager への到達可能性を監視する SIP オプション要求キープアラブを設定します。次に例を示します。

```
voice class sip-options-keepalive 101
  up-interval 30
  retry 3
  transport tcp
```

Options keepalive under dialpeer

```
dial-peer voice 101 voip
  description **CUCM/PBX**
  voice-class sip options-keepalive profile 101
```

- ダイヤルピアグループを設定するための関連 CLI コマンドは次のとおりです。
 - **voice class dpg dial-peer-group-id** (ダイヤルピアグループを作成します。)
 - **destination dpg dial-peer-group-id** (発信ダイヤルピアを選択するダイヤルピアグループを指定します。)
- サービスプロバイダールータを指示する SIP トランクダイヤルピア上にダイヤルピアグループを設定しないようにします。

- Unified Communications Manager を指示するダイヤルピア上で、宛先パターン(.T)を設定します。
- Unified Communications Manager の SIP トランク用の着信ダイヤルピアを指示するダイヤルピア上で、CLI コマンド **destination dpg dial-peer-group-id**(destination dpg 101)を設定します。この構成には、サービス プロバイダーを指示するダイヤルピア情報があります。
- ダイヤルピアからサービス プロバイダーへの **incoming called-number (.T)** は設定しないでください。SIP トランクからの着信コールは、着信者番号(.T)を削除した後に、ダイヤルピアアドレス情報「From URI」を使用して一致させます。

```
voice class uri 201 sip
host dns:sip-trunk.sample
```

```
Under dial-peer:
incoming uri from 201
```

- CLI コマンド **transport tcp tls v1.2** は、**voice class tenant** ではなく、**sip-ua** 設定モードの下に設定します。
 - セキュア SIP から SIP への(およびその逆の)コールフローでは連絡先ヘッダーを変更しないでください。そのようにすると、コールの確立で問題が生じることになります。SIP REQUESTS と RESPONSES 内のヘッダー情報を sips: から sip: に変更するために sip-profile を使用する場合、連絡先ヘッダーに「transport=tls」を含めるというルールが必要です。
 - ダイヤルピアが **voice class codec** を使用している場合、同じ **voice class codec** を **voice register pool** の下でも設定します。
 - srtp voice-class が **voice class srtp-crypto crypto-tag** コマンドを使用して作成されていることを確認します。サンプル設定を次に示します。
- ```
voice class srtp-crypto 1
crypto 1 AES_CM_128_HMAC_SHA1_32
crypto 2 AES_CM_128_HMAC_SHA1_80
```
- SIP レジストラについて **voice service voip sip** 設定モードの下で、着信登録の最大および最小有効期間を CLI コマンド **registrar server [expires [max sec] [min sec]]** を使用して設定します。
    - registrar server expires max 120 min 60**
  - SIP バインド機能に関連するすべての CLI コマンドを、**voice class tenant** 設定モードの下に移動させます。たとえば、CLI コマンド **voice-class sip bind control**、および **voice-class sip bind media** を、**voice class tenant** 設定モードの下で指定することをお勧めします。
  - NAT がルータ上で設定されている場合は、NAT サービスから SIP ポートを除外します。NAT サービスから SIP ポートを除外するための推奨 CLI は次のとおりです。
    - no ip nat service sip udp port 5060**
    - no ip nat service sip tcp port 5060**
  - CLI コマンドの **no supplementary-service sip refer**、**no supplementary-service sip moved-temporarily**、**supplementary-service media-renegotiate** を、**voice service voip** 設定モードで設定します
  - Unified SRST と Unified Border Element のコロケーション導入の場合は、CLI コマンド **no transport udp** を **sip-ua** 設定モードの下に設定しないでください。その理由は、電話機は非セキュア SIP SRST 設定でのシグナリング転送用に、UDP を使用して Unified SRST に登録されるためです。
  - メディア非アクティビティ タイマーを設定して、設定可能な期間内にリアルタイム プロトコル(RTP)パケットが受け取られなかった場合に、ルータがコールを監視して切断できるようにします。サンプル設定を次に示します。

```

ip rtcp report interval 9000
gateway
 media-inactivity-criteria all
 timer receive-rtp 1200
 timer receive-rtcp 5

```

## 制限事項

次の制約事項は、Unified SRST と Unified Border Element のコロケーション導入で順守されます。

- SIP トランク側の NAT ファイアウォール サポートは、CLI コマンド **no ip nat service sip udp port 5060** および **no ip nat service sip tcp port 5060** を使用して無効にする必要があります。
- Unified SRST と Unified Border Element のコロケーション導入では、一部の SIP トランクの機能はサポートされません。サポート対象の機能のリストについては、[Unified SRST と Unified Border Element のコロケーション](#)を参照してください。

## 例

次に、音声クラス テナントの設定例を示します。

```

voice class tenant 1
 registrar ipv4:10.0.0.1:5061 scheme sips expires 240 tcp tls auth-realm sip-trunk.sample
 credentials number +492281844672 username xxxx password xxxx realm sip-trunk.sample
 authentication username xxxx password xxxx realm sip-trunk.sample
 no remote-party-id
 timers expires 900000
 timers register 100
 sip-server dns:sip-trunk.sample:5061
 connection-reuse
 asserted-id pai
 bind control source-interface GigabitEthernet0/0/1
 bind media source-interface GigabitEthernet0/0/1
 conn-reuse
 sip-profiles 3000
 outbound-proxy dns:reg.sip-trunk.sample
 privacy-policy passthru
 call-route p-called-party-id
 midcall-signaling preserve-codec

```

次の設定では、前の例で設定された音声クラス テナントは、SIP トランク上のダイヤルピアの一部です。

```

dial-peer voice 201 voip
 description **SIP-TRUNK.SAMPLE**
 session protocol sipv2
 session target sip-server
 session transport tcp tls
 destination e164-pattern-map 201
 incoming uri from 201
 voice-class codec 1
 voice-class sip url sips
 voice-class sip asserted-id pai
 voice-class sip outbound-proxy dns:reg.sip-trunk.sample
 voice-class sip tenant 1
 voice-class sip srtp-crypto 1
 voice-class sip bind control source-interface GigabitEthernet0/0/1
 voice-class sip bind media source-interface GigabitEthernet0/0/1
 dtmf-relay rtp-nte
 srtp
 fax-relay ecm disable

```

```

fax rate 14400
ip qos dscp cs6 signaling
clid strip name
no vad

```

次の例は、Unified SRST と Unified Border Element のコロケーション導入に対する **show running-config** コマンドの出力を示しています。

Building configuration...

```

Current configuration : 15564 bytes
!
! Last configuration change at 17:52:50 IST Tue Jul 4 2017
! NVRAM config last updated at 17:52:54 IST Tue Jul 4 2017
!
version 16.7
service timestamps debug datetime msec
service timestamps log datetime msec
service sequence-numbers
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
platform shell
platform trace runtime slot F0 bay 0 process forwarding-manager module aom level debug
platform trace runtime slot F0 bay 0 process forwarding-manager module dsp level verbose
platform trace runtime slot F0 bay 0 process forwarding-manager module sbc level debug
platform trace runtime slot R0 bay 0 process forwarding-manager module dsp level verbose
platform trace runtime slot R0 bay 0 process forwarding-manager module om level debug
platform trace runtime slot R0 bay 0 process forwarding-manager module sbc level debug
!
hostname be4k-technium
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
! card type command needed for slot/bay 0/1
no logging queue-limit
logging buffered 100000000
no logging rate-limit
no logging console
!
no aaa new-model
process cpu statistics limit entry-percentage 10 size 7200
clock timezone IST 5 30
!
!
!
ip host gauss-lnx.cisco.com 10.0.0.1
ip name-server 10.0.0.1
ip dhcp excluded-address 10.0.0.1 10.0.0.2
!
ip dhcp pool phones
network 10.0.0.1 255.255.0.0
default-router 10.0.0.1
domain-name cisco.com

```

```

dns-server 10.0.0.1
!
subscriber templating
!
multilink bundle-name authenticated
!
!
trunk group 1
 xsvc
!
!
crypto pki trustpoint siggw1
 enrollment url http://10.0.0.1:80
 serial-number
 ip-address 10.0.0.1
 subject-name CN=siggw1
 revocation-check crl
 rsakeypair cisco123
!
crypto pki certificate chain siggw1
certificate 02
 30820234 3082019D A0030201 02020102 300D0609 2A864886 F70D0101 05050030
 13311130 0F060355 04031308 63617365 72766572 301E170D 31373036 32383134
 32393330 5A170D31 38303632 38313432 3933305A 305C310F 300D0603 55040313
 06736970 67773131 49301206 03550405 130B4644 4F323031 31413132 33301706
 092A8648 86F70D01 0908130A 382E3339 2E32332E 3133301A 06092A86 4886F70D
 01090216 0D626534 6B2D7465 63686E69 756D3081 9F300D06 092A8648 86F70D01
 01010500 03818D00 30818902 818100B5 3CE45902 52517DBE E735F0B5 9D6A412F
 FBF398A8 F306F28F A4C79A41 198A19D7 06025696 F5EC6237 EFCB1BBD C7430263
 1D0D3C7E AF06B4B2 0D30547C F049A3CD CC4FCFA1 335DA8C5 602A2D18 F91ECC32
 E0A7E279 60945941 DF5B53F9 102B9067 8782C1E0 874D6CBC DB0CDA82 C64B7423
 E56C5C33 2E13C729 9AB7FEEA 068E7102 03010001 A34F304D 300B0603 551D0F04
 04030205 A0301F06 03551D23 04183016 8014265B 6595680C E517CC42 F54AE9EC
 1F328FBE BF33301D 0603551D 0E041604 14BA096E DE4E2289 12E8F4D8 95E06E4A
 F93876E7 96300D06 092A8648 86F70D01 01050500 03818100 9B172FF6 291C193A
 E505ABE9 45AC3202 621BBE2B 6BA45F19 AE0DA7A0 EF5FBC19 5197094E 7A50BCF3
 CC49656E AOD991AC FED14749 EAB50892 0239E39C 345ED555 7CD74760 66B0DF49
 7E26B654 B8F9E1B1 72FD4039 8A13C9AC EBE75F21 B457D8E3 24BA70E3 F1B3A0C9
 5C3153FA B3C744B7 D81F706F B836617F 9E95AD51 813F20AD
quit
certificate ca 01
 308201FF 30820168 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 13311130 0F060355 04031308 63617365 72766572 301E170D 31373036 32383134
 32383131 5A170D32 30303632 37313432 3831315A 30133111 300F0603 55040313
 08636173 65727665 7230819F 300D0609 2A864886 F70D0101 01050003 818D0030
 81890281 8100A3AC A4003239 62667AB4 6E8ACE2B 90672DD8 1E2A2952 AFC8A1F6
 D56173C9 269F9176 747E93D1 6F699B6F 0C2E600D 8C864F27 4379ED8A E88187F7
 17A77C63 B87B7EF6 1556D949 43C743F6 01D9941D 946FCEC8 880B342C 97CC9CEA
 9F015EAC A667F30B 505281AA 29EB10A3 F1C75A99 2A224653 F3B985DD F17BC8DD
 40C8C609 62C90203 010001A3 63306130 0F060355 1D130101 FF040530 030101FF
 300E0603 551D0F01 01FF0404 03020186 301F0603 551D2304 18301680 14265B65
 95680CE5 17CC42F5 4AE9EC1F 328FBEBF 33301D06 03551D0E 04160414 265B6595
 680CE517 CC42F54A E9EC1F32 8FBEBF33 300D0609 2A864886 F70D0101 04050003
 81810077 C36A6C9A B7C18856 EBDA4504 C38565F0 CF6385EE 29AFC38B 8B90C741
 B20C8C36 E979FD72 7B849B34 0BBE3EFA 191E1776 C28FDCFB 5D5F7CFF 170CF615
 B4105ABD CD6E0318 4B576FFD 44D115FF 2817E279 78B2794E 577F694F DD129820
 B500BB08 E57BFAA9 87835645 4EA53352 B80B51AD 2CC0633A AB9974EB E523A944 0EC230
quit
!
voice service voip
 ip address trusted list
 ipv4 10.0.0.1 255.255.0.0
 ipv4 10.0.0.1 255.0.0.0
 address-hiding

```

```

mode border-element license capacity 50
media statistics
media bulk-stats
media disable-detailed-stats
allow-connections sip to sip
no supplementary-service sip moved-temporarily
no supplementary-service sip refer
supplementary-service media-renegotiate
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
sip
 registrar server expires max 240 min 60
!
voice class uri 101 sip
 host ipv4:10.0.0.1
!
voice class uri 201 sip
 host dns:sip-trunk.sample
!
voice class uri 301 sip
 host ipv4:10.0.0.1
voice class codec 1
 codec preference 1 g711alaw
 codec preference 2 g722-64
 codec preference 3 g711ulaw
!
voice class sip-profiles 3000
 rule 1 request REGISTER sip-header SIP-Req-URI modify "sips:(*)" "sip:\1"
 rule 2 request REGISTER sip-header To modify "<sips:(*)" "<sip:\1"
 rule 3 request REGISTER sip-header From modify "<sips:(*)" "<sip:\1"
 rule 4 request REGISTER sip-header Contact modify "<.*:.*@(.)>"
"<sip:\1;transport=tls;bnc>"
 rule 6 request REGISTER sip-header Proxy-Require add "Proxy-Require: gin"
 rule 7 request REGISTER sip-header Require add "Require: gin"
!
voice class sip-profiles 201
 rule 1 request ANY sip-header P-Asserted-Identity modify "<sips:(*)>"
"<sip:+4922842293220@sip-trunk.sample>"
 rule 2 request ANY sip-header SIP-Req-URI modify "sips:(*)" "sip:\1"
 rule 3 request ANY sip-header To modify "<sips:(*)" "<sip:\1"
 rule 4 request ANY sip-header From modify "<sips:(*)" "<sip:\1"
 rule 5 request ANY sip-header Contact modify "<sips:(*)>" "<sip:\1;transport=tls>"
 rule 6 response ANY sip-header To modify "<sips:(*)" "<sip:\1"
 rule 7 response ANY sip-header From modify "<sips:(*)" "<sip:\1"
 rule 8 response ANY sip-header Contact modify "<sips:(*)>" "<sip:\1;transport=tls>"
 rule 9 request ANY sip-header Min-SE remove
 rule 10 request ANY sip-header Diversion remove
 rule 11 request ANY sdp-header Connection-Info remove
 rule 12 response ANY sdp-header Connection-Info remove
 rule 13 request INVITE sip-header Allow-Header modify "INFO," ""
!
voice class sip-profiles 101
 rule 1 request INVITE sip-header Supported modify "100rel," ""
!
voice class sip-profiles 102
 rule 1 request INVITE sip-header Privacy add "Privacy:id"
 rule 2 request INVITE sip-header P-Called-Party-ID add "P-Called-Party-ID:
sip:2001@10.0.0.1"
!
!
voice class sip-copylist 201
 sip-header FROM
!
voice class e164-pattern-map 101
 e164 +492284229322T

```

```
!
!
voice class e164-pattern-map 201
 e164 11[02]
 e164 11[68]T
 e164 11[025]
 e164 +T
 e164 0T
 e164 2...
!
!
voice class e164-pattern-map 301
 e164 3...
!
!
voice class dpg 201
!
voice class dpg 101
 dial-peer 201
!
voice class dpg 301
 dial-peer 301
!
voice class server-group 1
 ipv4 10.0.0.1
 description **CUCM Server Group**
!
voice class sip-options-keepalive 101
 up-interval 30
 retry 3
 transport tcp
 sip-profiles 3000
!
voice class tenant 2
 registrar dns:sip-trunk.sample:5060 expires 240 tcp auth-realm sip-trunk.sample
 credentials number +492281844673 username abcd password xxxx realm sip-trunk.sample
 authentication username abcd password xxxx realm sip-trunk.sample
 no remote-party-id
 timers expires 900000
 timers register 100
 timers buffer-invite 10000
 timers dns registrar-cache ttl
 sip-server dns:sip-trunk.sample:5060
 connection-reuse
 asserted-id pai
 bind control source-interface GigabitEthernet0/0/1
 bind media source-interface GigabitEthernet0/0/1
 no pass-thru content custom-sdp
 conn-reuse
 sip-profiles 3000
 outbound-proxy dns:reg.sip-trunk.sample
 privacy-policy passthru
 call-route p-called-party-id
 midcall-signaling preserve-codec
!
voice class tenant 4
 timers expires 60000
 timers buffer-invite 10000
 connection-reuse
 asserted-id pai
 bind control source-interface GigabitEthernet0/0/0
 bind media source-interface GigabitEthernet0/0/0
 no pass-thru content custom-sdp
 privacy-policy passthru
```

```

 call-route p-called-party-id
 midcall-signaling preserve-codec
!
voice class tenant 1
 registrar dns:sip-trunk.sample:5061 scheme sips expires 240 tcp tls auth-realm
sip-trunk.sample
 credentials number +492281844672 username abcd password xxxx realm sip-trunk.sample
 authentication username abcd password xxxx realm sip-trunk.sample
 no remote-party-id
 timers expires 60000
 timers register 100
 timers buffer-invite 1000
 timers dns registrar-cache ttl
 sip-server dns:sip-trunk.sample:5061
 connection-reuse
 asserted-id pai
 bind control source-interface GigabitEthernet0/0/1
 bind media source-interface GigabitEthernet0/0/1
 no pass-thru content custom-sdp
 conn-reuse
 sip-profiles 3000
 outbound-proxy dns:reg.sip-trunk.sample
 privacy-policy passthru
 call-route p-called-party-id
 midcall-signaling preserve-codec
!
voice class tenant 3
 registrar dns:sipp.sample:6600 expires 240 auth-realm sip-trunk.sample
 credentials number +492281844672 username abcd password xxxx realm sip-trunk.sample
 authentication username abcd password xxxx realm sip-trunk.sample
 no remote-party-id
 timers expires 900000
 timers register 500
 timers buffer-invite 1000
 timers dns registrar-cache ttl
 sip-server dns:sipp.sample
 connection-reuse
 asserted-id pai
 bind control source-interface GigabitEthernet0/0/1
 bind media source-interface GigabitEthernet0/0/1
 no pass-thru content custom-sdp
 conn-reuse
 sip-profiles 3000
 outbound-proxy dns:sipp.sample:6600
 privacy-policy passthru
 call-route p-called-party-id
 midcall-signaling preserve-codec
!
voice class srtp-crypto 1
 crypto 1 AES_CM_128_HMAC_SHA1_32
 crypto 2 AES_CM_128_HMAC_SHA1_80
!
!
!
voice register global
 default mode
 no allow-hash-in-dn
 max-dn 40
 max-pool 40
!
voice register pool 1
 id network 8.55.0.0 mask 255.255.0.0
 dtmf-relay rtp-nte
 voice-class codec 1

```



```
!
voice hunt-group 1 parallel
 list 1001,1002,1003
 timeout 15
 statistics collect
 pilot 1234
!
!
voice hunt-group 2 sequential
 list 1002,1003,1004
 timeout 5
 statistics collect
 pilot 2345
!
voice-card 0/1
 dsp services dspfarm
 no watchdog
!
license udi pid ISR4321/K9 sn FDO201115PV
license boot level uck9
license boot level securityk9
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
!
username abcd password xxxx
username abcd password xxxx
!
redundancy
 mode none
!
template 1
!
!
!
!
interface GigabitEthernet0/0/0
 ip address 10.0.0.1 255.255.0.0
 ip nat inside
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.0.0
 ip nat outside
 negotiation auto
!
interface Service-Engine0/1/0
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 negotiation auto
!
no ip nat service sip tcp port 5060
no ip nat service sip udp port 5060
ip nat pool pool1 10.0.0.1 10.255.255.255 netmask 255.255.0.0
ip nat inside source list 100 interface GigabitEthernet0/0/1 overload
ip forward-protocol nd
ip http server
```

```

no ip http secure-server
ip tftp source-interface GigabitEthernet0/0/0
ip tftp blocksize 1520
ip rtcp report interval 9000
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 10.0.0.1 255.0.0.0 10.0.0.1
!
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
!
ip access-list extended nat-list
access-list 100 permit ip 10.0.0.1 255.255.0.0 any
!
!
tftp-server flash:fbi88xx.BE-01-010.sbn
tftp-server flash:kern88xx.12-0-1MN-113.sbn
tftp-server flash:rootfs88xx.12-0-1MN-113.sbn
tftp-server flash:sb288xx.BE-01-020.sbn
tftp-server flash:sip88xx.12-0-1MN-113.loads
tftp-server flash:vc488xx.12-0-1MN-113.sbn
!
!
ipv6 access-list preauth_v6
permit udp any any eq domain
permit tcp any any eq domain
permit icmp any any nd-ns
permit icmp any any nd-na
permit icmp any any router-solicitation
permit icmp any any router-advertisement
permit icmp any any redirect
permit udp any eq 547 any eq 546
permit udp any eq 546 any eq 547
deny ipv6 any any
!
control-plane
!
voip trunk group 1
 xsvc
!
uc wsapi
 message-exchange max-failures 99
 response-timeout 2
 source-address 10.0.0.1
 probing interval keepalive 60
 probing max-failures 2
 provider xcc
 remote-url http://10.0.0.1:8090/xcc
 !
 provider xsvc
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!
!
dial-peer voice 201 voip
 description **SIP-TRUNK.SAMPLE**
 session protocol sipv2

```

```
session target sip-server
session transport tcp tls
destination e164-pattern-map 201
incoming uri from 201
voice-class codec 1
voice-class sip url sips
voice-class sip profiles 201
voice-class sip tenant 1
voice-class sip srtp-crypto 1
dtmf-relay rtp-nte
srtp
fax-relay ecm disable
fax rate 14400
clid strip name
no vad
!
dial-peer voice 301 voip
description **SIP-TRUNK.SAMPLE**
session protocol sipv2
session target sip-server
session transport tcp
destination e164-pattern-map 301
incoming uri from 201
voice-class codec 1
voice-class sip url sip
voice-class sip profiles 201
voice-class sip tenant 2
dtmf-relay rtp-nte
srtp fallback
fax-relay ecm disable
fax rate 14400
clid strip name
no vad
!
dial-peer voice 401 voip
description **SIP-TRUNK.SAMPLE**
destination-pattern 4...
session protocol sipv2
session target sip-server
session transport udp
incoming uri from 301
voice-class codec 1
voice-class sip url sip
voice-class sip profiles 201
voice-class sip tenant 3
dtmf-relay rtp-nte
fax-relay ecm disable
fax rate 14400
clid strip name
no vad
!
dial-peer voice 101 voip
description **CUCM/PBX**
destination-pattern .T
session protocol sipv2
session transport tcp
session server-group 1
destination dpg 101
incoming uri via 101
voice-class codec 1
no voice-class sip outbound-proxy
voice-class sip srtp negotiate cisco
voice-class sip profiles 102 inbound
voice-class sip tenant 4
```

```

voice-class sip srtp-crypto 1
voice-class sip options-keepalive profile 101
dtmf-relay rtp-nte
srtp fallback
fax-relay ecm disable
fax rate 14400
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback pass-through g711alaw
no vad
!
!
presence
!
gateway
media-inactivity-criteria all
timer receive-rtcp 5
timer receive-rtp 180
!
sip-ua
transport tcp tls v1.2
crypto signaling default trustpoint sipgw1
!
alias exec cl clear logg
alias exec rtp show voip rtp connections
alias exec pool show voice register pool all brief
!
line con 0
exec-timeout 0 0
password xxxx
width 0
transport input none
stopbits 1
line aux 0
stopbits 1
line vty 0 4
exec-timeout 0 0
password xxxx
login local
length 0
transport input all
!
end

```

## Unified SRST での SIP トランキングの設定についての機能情報

表 9-1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォームのサポート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検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、Cisco IOS および Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator にアクセスするには、<http://www.cisco.com/go/cfn> に移動します。Cisco.com のアカウントは必要ありません。



(注) 表には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連の Cisco IOS ソフトウェア リリースでもサポートされます。

表 9-1 Unified SRST での SIP トランキングの設定についての機能情報

| 機能名                                            | リリース                     | 機能情報                                                                                       |
|------------------------------------------------|--------------------------|--------------------------------------------------------------------------------------------|
| Unified SRST と Unified Border Element のコロケーション | Cisco IOS XE Fuji 16.7.1 | Cisco 4000 シリーズ サービス統合型ルータ上での Unified SRST と Unified Border Element のコロケーションのサポートが追加されました。 |





## ボイスメールと Cisco Unified SRST の統合

この章では、Cisco Unified Communications Manager のフォールバック中に、既存のボイスメールシステムを Cisco Unified SRST ルータに接続されている電話機に実装する方法を説明します。

Cisco Unified SRST は、Cisco Unified IP Phone やルータ音声ゲートウェイの音声ポートとやり取りする Session Initiation Protocol (SIP) の着信コールと発信コールもサポートします。SIP は Cisco Unified SRST ルータが PSTN ゲートウェイから分離していて、SRST と PSTN ゲートウェイが (H.323 ではなく) SIP を使用してリンクされている状況で使用されます。

SIP の詳細については、『[Cisco IOS SIP Configuration Guide](#)』を参照してください。

### 目次

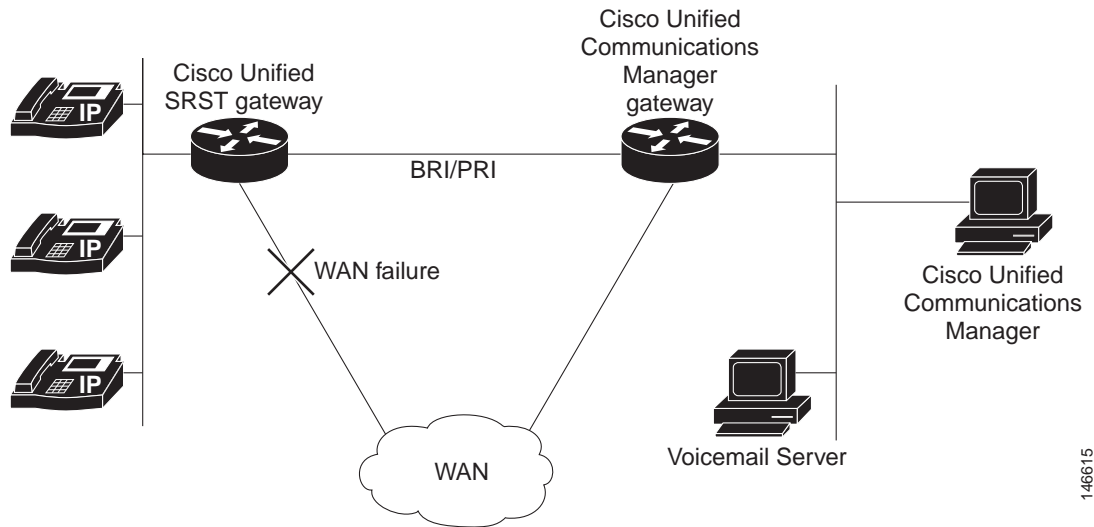
- [ボイスメールの統合について Cisco Unified SRST \(243 ページ\)](#)
- [ボイスメールと Cisco Unified SCCP および SIP SRST との統合方法 \(245 ページ\)](#)
- [メッセージ待機インジケータの設定 \(SRST モードの SIP 電話\) \(257 ページ\)](#)
- [SIP アプリケーションとボイスメールに DTMF リレーを設定する方法 \(262 ページ\)](#)
- [次の作業 \(265 ページ\)](#)

## ボイスメールの統合について Cisco Unified SRST

Cisco Unified SRST は、Cisco Unified CM のフォールバック中に Cisco Unity および他のボイスメールシステムからボイスメールメッセージの送受信を行うことができます。WAN がダウンしたとき、BRI または PRI によって Cisco Unified SRST システムにアクセスできるボイスメールシステムは、ISDN シグナリングを使用します (図 10-1 を参照)。Foreign Exchange Office (FXO) または Foreign Exchange Station (FXS) によって PSTN にアクセスできるシステムは、インバンドデュアルトーン多重周波数 (DTMF) シグナリングを使用します (図 10-2 を参照)。

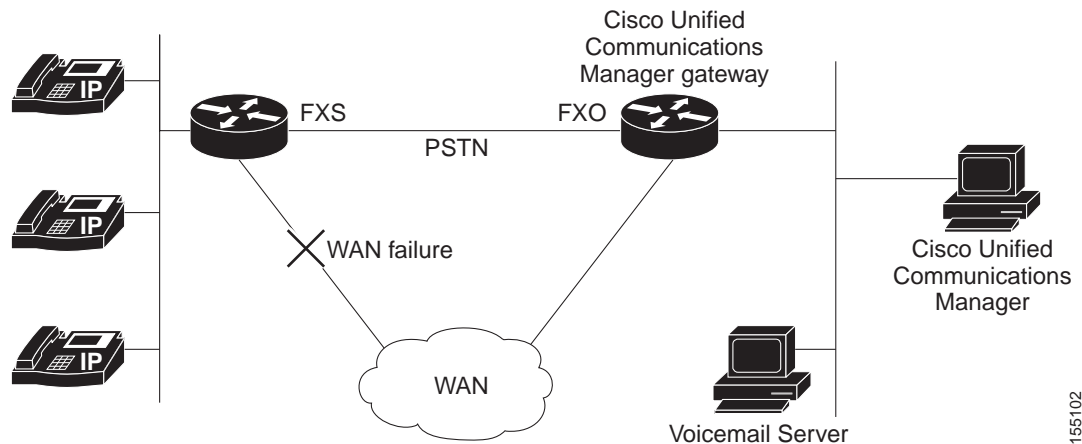
Unified SRST リリース 12.0 以降、Unified SRST は SIP IP Phone 用の IPv6 プロトコルでボイスメールをサポートしています。

図 10-1 BRI または PRI での Cisco Unified Communications Manager のフォールバック



146615

図 10-2 PSTN での Cisco Unified Communications Manager のフォールバック



155102

どちらの設定でも、電話機のメッセージ ボタンはアクティブのまま、話中または無応答の番号へのコールは、ダイヤルした番号のメールボックスに転送されます。

話中信号を受けたコール、無応答コール、およびメッセージ ボタンを押して開始されたコールは、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、話中と無応答のコール用、およびメッセージ ボタン用にボイスメール システムへのルーティングを設定する必要があります。

ボイスメール システムが FXO または FXS 経由でアクセスされる場合、適切なボイスメール 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 システムに指示 (DTMF パターン) を設定する必要があります。ボイスメール システムが BRI または PRI 経由でアクセスされる場合、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、指示を設定する必要はありません。



# ボイスメールと Cisco Unified SCCP および SIP SRST との統合方法

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\(245 ページ\)](#) (必須)
- [メッセージ ボタンの設定\(248 ページ\)](#) (必須)
- [Cisco Unified Communications Manager ゲートウェイへのリダイレクト\(250 ページ\)](#) (BRI または PRI で必須)
- [ボイスメールへのコール転送の設定\(251 ページ\)](#) (FXO または FXS で必須)
- [メッセージ待機インジケータの設定\(Cisco Unified SRST ルータ\) \(255 ページ\)](#) (任意)



(注) SIP SRST のサポートは、IOS リリース 15.1(4)M3 および 15.2(1)T2 から追加されています。

## ボイスメールへのダイレクトアクセスの設定

BRI/PRI または FXO/FXS を使用して、ボイスメール システムへの直接アクセスを設定できます。BRI/PRI または FXO/FXS のアクセスでボイス メール メッセージにアクセスするには、ボイス メール システムの番号に一致する接続先パターンで設定されている POTS ダイアル ピアが必要です。また、ボイスメール システムがアクセスできるポートとダイアル ピアを関連付ける必要があります。

設定の両方のセットは、ダイアルピア設定モードで行われます。以下に示す概要と詳細な手順には、この作業を実行するために必要な基本的なコマンドだけが記載されています。特定のダイアルピア設定では、追加のコマンドが必要となる場合があります。

### 手順の概要

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`

## 手順の詳細

|      | コマンドまたはアクション                                                                                                                  | 目的                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 1 | <pre>dial-peer voice tag {pots   voatm   vofr   voip}</pre> <p>例:<br/>Router(config)# dial-peer voice 1002 pots</p>           | <p>(FXO または FXS、および BRI または 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て、ダイヤルピア コンフィギュレーション モードを開始します。</p> <p><b>dial-peer</b> コマンドは、各ルータで異なる構文を示します。この例は、Cisco 3600 シリーズ ルータの構文を示します。</p> <ul style="list-style-type: none"> <li>• <b>tag</b>: 特定のダイヤルピアを定義する番号。範囲は 1 ~ 2147483647 です。</li> <li>• <b>pots</b>: 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>• <b>voatm</b>: 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>• <b>vofr</b>: 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>• <b>voip</b>: 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> |
| 手順 2 | <pre>destination-pattern [+] string [T]</pre> <p>例:<br/>Router(config-dial-peer)# destination-pattern 1100T</p>               | <p>(FXO または FXS、および BRI または PRI) (ダイヤルプランに応じて) 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。</p> <ul style="list-style-type: none"> <li>• <b>+</b>: (任意) E.164 の標準的な番号を示す文字。</li> <li>• <b>string</b>: 表 10-1 を参照してください。</li> <li>• <b>T</b>: (任意) 接続先パターンの値が可変長のダイヤル文字列であることを示す制御文字。</li> </ul>                                                                                                                                                                                                                                                                                                                                    |
| 手順 3 | <pre>port {slot-number/subunit-number/port   slot/port:ds0-group-no}</pre> <p>例:<br/>Router(config-dial-peer)# port 1/1/1</p> | <p>(FXO または FXS、および BRI または PRI) Cisco ルータ上の特定の音声ポートとダイヤルピアを関連付けます。</p> <ul style="list-style-type: none"> <li>• <b>slot-number</b>: 音声インターフェイス カード (VIC) がインストールされているルータのスロット番号。有効なエントリは、インストールされているスロットに応じて 0 ~ 3 です。</li> <li>• <b>subunit-number</b>: 音声ポートが配置されている 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>• <b>port</b>: 音声ポート番号。有効なエントリは 0 および 1 です。</li> <li>• <b>ds0-group-no</b>: DS0 グループ番号を指定します。定義済みの DS0 グループ番号はそれぞれの音声ポート上に表示されています。これによって、デジタル T1/E1 カード上で個々の DS0 を定義できます。</li> </ul>                                                                                                                          |

| コマンドまたはアクション                                                                                                                              | 目的                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>手順 4 <code>forward-digits {num-digit   all   extra}</code></p> <p>例:<br/>Router(config-dial-peer)# <code>forward-digits all</code></p> | <p>(FXO または FXS では任意) 音声コールに対して転送される桁を指定します。</p> <ul style="list-style-type: none"> <li>• <b>num-digit</b>: 転送する桁数。桁数が接続先電話番号の長さを超えている場合、接続先電話番号の長さを使用されます。範囲は 0 ~ 32 です。値を 0 に設定すると、<b>no forward-digits</b> コマンドを入力した場合と同じ結果が得られます。</li> <li>• <b>all</b>: すべての桁を転送します。<b>all</b> を入力すると、接続先パターンの長さ全体が使用されます。</li> <li>• <b>extra</b>: ダイヤルした数字列の長さがダイヤルピアの接続先パターンよりも大きければ、右揃えした追加の桁が転送されます。ただし、ダイヤルピアの接続先パターンが可変長で、文字「T」で終了している (例:T、123T、123...T) 場合は、追加の桁は転送されません。</li> </ul> |
| <p>手順 5 <code>exit</code></p> <p>例:<br/>Router(config-dial-peer)# <code>exit</code></p>                                                   | <p>(FXO または FXS、および BRI または PRI) ダイヤルピアコンフィギュレーション モードを終了します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                  |

表 10-1 destination-pattern コマンドの文字列引数で有効なエントリ

| 入力                     | 説明                                                                                                        |
|------------------------|-----------------------------------------------------------------------------------------------------------|
| 数字の 0 ~ 9              | —                                                                                                         |
| A ~ D の文字              | —                                                                                                         |
| アスタリスク (*) とシャープ記号 (#) | これらは標準のプッシュトーン ダイヤルパッドで表示されます。                                                                            |
| カンマ (,)                | 数字の間に区切りを挿入します。                                                                                           |
| ピリオド (.)               | 入力した任意の数字に一致します (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 (%)            | 先行する数字がゼロ回以上出現したことを示します。ワイルドカードでの使い方と同様です。                                                                |
| プラス記号 (+)              | 先行する数字が 1 回以上出現したことを示します。<br>(注) 数字列の一部として使用されるプラス記号は、文字列が標準の E.164 番号であることを示すために数字列の前に使用できるプラス記号とは異なります。 |
| キャレット (^)              | 文字列の先頭との一致を示します。<br>カッコ ( ( ) )、パターンを示し、正規表現の規則と同じです。                                                     |
| ドル記号 (\$)              | 入力文字列の末尾のヌルストリングと一致します。                                                                                   |
| バックスラッシュ記号 (\)         | 単一の文字に続き、その文字と一致します。他の意味がない単一の文字とともに使用できます (その文字と一致します)。                                                  |
| 疑問符 (?)                | 先行する数字がゼロ回または 1 回出現したことを示します。                                                                             |
| 角カッコ ([ ])             | 範囲を示します。範囲は角カッコで囲まれた文字のシーケンスであり、この範囲では 0 ~ 9 の数字だけが許可されます。                                                |

## 例

次の FXO および FXS の例は、名前付き POTS ダイアルピア 1102 を設定し、ダイアルピア 1102 がボイスメールの内線番号 1101 に一致させ、ダイアルピア 1102 をボイスメール システムが接続される音声ポート 1/1/1 に割り当てます。他のダイアルピアはボイスメールに直接アクセスするように設定されます。

```
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、POTS ダイアルピア 1102 がポート 2/0:23 を通って直接 1101 に移動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 のフォールバック中に、Cisco Unified SCCP および SIP SRST ルータに接続された Cisco Unified IP Phone のメッセージ ボタンを有効にするには、ボイスメール システムにスピードダイヤル番号をプログラムする必要があります。スピードダイヤル番号は、Cisco Unified CM のフォールバック中に、Cisco Unified SCCP および SIP SRST ルータに接続されている電話機のメッセージ ボタンが押された時にダイヤルされます。また、話中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、コール転送を設定する必要があります。

この設定は FXO または FXS と、BRI または PRI で必要です。

## 手順の概要

1. **call-manager-fallback**
2. **voicemail phone-number**
3. **call-forward busy directory-number**
4. **call-forward noan directory-number timeout seconds**
5. **exit**
6. **voice register pool tag**
7. **call-forward b2bua busy directory-number**
8. **call-forward b2bua noan directory-number timeout seconds**
9. **exit**

## 手順の詳細

|      | コマンドまたはアクション                                                                                                                         | 目的                                                                                                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 1 | <b>call-manager-fallback</b><br><br>例:<br>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。                                                                                                                                                                                                                                |
| 手順 2 | <b>voicemail phone-number</b><br><br>例:<br>Router(config-cm-fallback)# voicemail 5550100                                             | Cisco Unified IP SCCP 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。<br><br>• <i>phone-number</i> : メッセージを取得するためのスピードダイヤル番号として設定される電話番号。                                                                                                                                        |
| 手順 3 | <b>call-forward busy directory-number</b><br><br>例:<br>Router(config-cm-fallback)# call-forward busy 2000                            | Cisco SCCP IP Phone が話中のときに行われる別の番号へのコール転送を設定します。<br><br>• <i>directory-number</i> : 完全修飾 E.164 番号を表す選択された電話番号。この番号には、電話の内線番号内で右揃えした桁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。                                                                                                          |
| 手順 4 | <b>call-forward noan directory-number timeout seconds</b><br><br>例:<br>Router(config-cm-fallback)# call-forward noan 2000 timeout 10 | Cisco SCCP IP Phone から応答を受信しなかった場合の別の番号へのコール転送を設定します。<br><br>• <i>directory-number</i> : 完全修飾 E.164 番号を表す選択された電話番号。この番号には、電話の内線番号内で右揃えした桁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。<br><br>• <b>timeout seconds</b> : コールが別の電話に転送されるまでの待ち時間を秒単位で設定します。 <i>seconds</i> の範囲は 3 ~ 60000 です。 |
| 手順 5 | <b>exit</b><br><br>例:<br>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。                                                                                                                                                                                                                                |

|      | コマンドまたはアクション                                                                                                                          | 目的                                                                                                                                                                                                                                                                                                                      |
|------|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 6 | voice register pool tag<br><br>例:<br>Router(config)# voice register pool 1                                                            | 音声レジスタ プール コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                                                       |
| 手順 7 | call-forward b2bua busy directory-number<br><br>例:<br>Router(config-register-pool)# call-forward b2bua busy 2000                      | Cisco SIP IP Phone が話中のときに行われる別の番号へのコール転送を設定します。<br><br><ul style="list-style-type: none"> <li><i>directory-number</i>: 完全修飾 E.164 番号を表す選択された電話番号。この番号には、電話の内線番号内で右揃えした桁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>                                                                                                        |
| 手順 8 | call-forward b2bua noan directory-number timeout seconds<br><br>例:<br>Router(config-register-pool)# call-forward noan 2000 timeout 10 | Cisco SIP IP Phone から応答を受信しなかった場合の別の番号へのコール転送を設定します。<br><br><ul style="list-style-type: none"> <li><i>directory-number</i>: 完全修飾 E.164 番号を表す選択された電話番号。この番号には、電話の内線番号内で右揃えした桁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><i>timeout seconds</i>: コールが別の電話に転送されるまでの待ち時間を秒単位で設定します。<i>seconds</i> の範囲は 3 ~ 60000 です。</li> </ul> |
| 手順 9 | exit<br><br>例:<br>Router(config-register-pool)# exit                                                                                  | 音声レジスタ プール 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 のメッセージ ボタンが押された時に発行されるスピードダイヤル番号として、1101 を指定します。話中および無応答のコールはすべて、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
voice register pool 1
 call-forward b2bua busy 1101
 call-forward b2bua 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 経由でアクセスするボイスメールシステムでは、以下のタスクが必要です。

Cisco Unified SRST は、個人メッセージを取得するメッセージ ボタンのサポートに加えて、話中および無応答の番号へのコールをボイスメール システムに自動転送する機能をサポートします。BRI または PRI 経由でアクセスされるボイスメール 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することができます。そのためには、Cisco Unified CM の一部の設定が推奨されます。お使いのボイスメール システムがリダイレクトされた着信番号識別サービス (RDNIS) をサポートする場合、Cisco Unified CM へ発信するセットアップ メッセージに RDNIS を含め、設定されたデバイスとアプリケーション間でやり取りされた、最後にリダイレクトされた番号と最初にダイヤルした番号を宣言する必要があります。

- 
- 手順 1 Cisco Unified CM の任意のページから、[デバイス (Device)] および [ゲートウェイ (Gateway)] をクリックします。
- 手順 2 [ゲートウェイの検索と一覧表示 (Find and List Gateways)] ページで、[検索 (Find)] をクリックします。
- 手順 3 [ゲートウェイの検索と一覧表示 (Find and List Gateways)] ページでデバイス名を選択します。
- 手順 4 [ゲートウェイ設定 (Gateway Configuration)] ページで、[番号 IE 配信のリダイレクト - 発信 (Redirecting Number IE Delivery - Outgoing)] をチェックします。
- 

## ボイスメールへのコール転送の設定



(注) FXO または FXS 経由でアクセスするボイスメール システムでは、以下のタスクが必要です。

Cisco Unified SRST は、個人メッセージを取得するメッセージ ボタンのサポートに加えて、話中または無応答の番号へのコールをボイスメール システムに自動転送する機能をサポートします。転送されたコールは、ボイスメール システムのほぼ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者番号のメールボックスに転送されます。

### DTMF デジジット パターンを使用したコールのルーティング方法

転送されたコールを正しいボイスメール ボックスに送信できるようにするには、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、ボイスメール システムが特定のボイスメールの場所にアクセスするために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る DTMF デジジットで構成されます。たとえば、ボイスメール システムは、発信者がメッセージを残すには次の操作が必要となるように設計することができます。

1. 中央ボイスメール番号(1101)をダイヤルして # を押す。
2. 内線番号(6000)をダイヤルして # を押す。
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メニュー オプションを選択する。

Cisco Unified SRST が話中または無応答の番号へのコールを内線 6000 のメールボックスに転送するには、1101#6000#2 のシーケンスを発行するようにプログラムする必要があります。図 10-3 に示すように、これは **voicemail** コマンドと **pattern** コマンドにより実行します。

図 10-3 Cisco Unified SRST でボイスメールのダイヤル シーケンス 1101#6000#2 を設定する方法

```

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

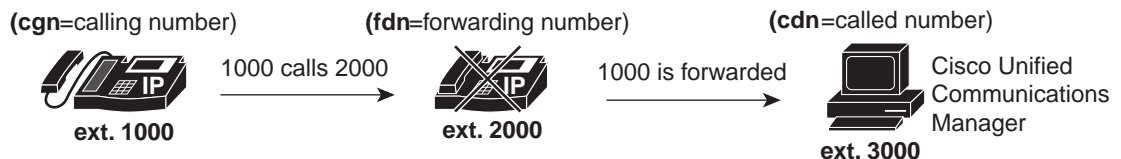
```

図 10-3 で示す **pattern** コマンドの # cgn #2、# cdn #2、および # fdn #2 の各部分は、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転送された着信コールの状態を宣言する 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 セットから 3 文字まで設定できます (A から D、0 から 9、# および \*)。ボイスメール システムが使用できる DTMF トーンのセットは限定されています。たとえば、Cisco Unity は A から 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、トークンのみの表示の前に星印 (\*) を配置した場合、「次のトークン番号をダイヤルする」ことを意味します。トークンの最後に配置されている場合、トークン番号の終わりを示すことができます。アスタリスクが他のタグ文字の間に配置されている場合、\* をダイヤルすることを意味します。タグの使用は、DTMF トーンがボイスメール システムによってどのように定義されているかによって異なります。

トークンは、コール転送チェーンのどの電話番号をパターンで使用するかを Cisco Unified SRST に示します。図 10-4 に示すように、ボイスメールの転送中に起こりうる 3 つのコール状態に対応して、3 つのタイプのトークンがあります。

図 10-4 番号をトークンから導出する方法



```

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

```

タグとトークンのセットまたはパターンは、次のいずれかが発生したときに、ボイスメール システムをアクティブ化します。

- ユーザが電話機のメッセージ ボタンを押す (**pattern direct** コマンド)。
- 内線番号から話中の内線に接続しようと試み、コールがボイスメールに転送される (**pattern ext-to-ext busy** コマンド)。
- 内線番号から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 (**pattern ext-to-ext no-answer** コマンド)。



- 外部トランク コールが話中の内線に到達し、コールがボイスメールに転送される (**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 (**pattern trunk-to-ext no-answer** コマンド)。

## 前提条件

- ボイスメール システムに FXO でヘアピン転送されたコールは、セントラル オフィスからの切断監視機能が必要です。詳細については、『*FXO Answer and Disconnect Supervision*』を参照してください。
- ボイスメール システムが正しく解釈でき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、DTMF トーンを解釈する方法を理解する必要があります (『*DTMF デジタル パターンを使用したコールのルーティング方法*』セクション(251 ページ)を参照)。

Cisco Unity がボイスメール コールをどのように処理しているかについては、『*How to Transfer a Caller Directly into a Cisco Unity Mailbox*』に記載されています。追加のコール処理情報については、『*Cisco Unity system administration guide*』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 ガイドや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。

## 手順の概要

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*]

## 手順の詳細

|      | コマンドまたはアクション                                                                                                                                                                                           | 目的                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 1 | <b>vm-integration</b><br><br>例:<br>Router(config)# vm-integration                                                                                                                                      | ボイスメール統合モードに入り、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実行できるようにします。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 手順 2 | <b>pattern direct tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</b><br><br>例:<br>Router(config-vm-int)# pattern direct 2 CGN *                                   | 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 デジタル パターンの転送を設定します。 <ul style="list-style-type: none"> <li>• <b>tag1</b>: 英数字の文字列で、長さが 4 桁未満の DTMF デジタル。この英数字文字列は、4 つの文字 (A、B、C、D)、2 つの記号 (*、#)、10 の数字 (0 ~ 9) で構成されます。タグの数字は、ボイスメールシステムの統合ファイルで、発信者番号、着信者番号、または転送番号のいずれかの直前で定義されている数字と照合されます。</li> <li>• <b>tag2</b> と <b>tag3</b>: (任意) <b>tag1</b> を参照してください。</li> <li>• <b>last-tag</b>: <b>tag1</b> を参照してください。このタグは、パターンの終わりを示します。</li> <li>• <b>CGN</b>: 発信者番号 (CGN) 情報がボイスメールシステムに送信されます。</li> <li>• <b>CDN</b>: 着信者番号 (CDN) 情報がボイスメールシステムに送信されます。</li> <li>• <b>FDN</b>: 転送番号 (FDN) 情報がボイスメールシステムに送信されます。</li> </ul> |
| 手順 3 | <b>pattern ext-to-ext busy tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</b><br><br>例:<br>Router(config-vm-int)# pattern ext-to-ext busy 7 FDN * CGN *           | 内線から話中の内線に接続が試行され、コールがボイスメールに転送されるときに、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 デジタル パターンの転送を設定します。引数およびキーワードの詳細については、 <a href="#">ステップ 2</a> を参照してください。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 手順 4 | <b>pattern ext-to-ext no-answer tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</b><br><br>例:<br>Router(config-vm-int)# pattern ext-to-ext no-answer 5 FDN * CGN * | 内線から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 デジタル パターンの転送を設定します。引数およびキーワードの詳細については、 <a href="#">ステップ 2</a> を参照してください。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|      | コマンドまたはアクション                                                                                                                                                                                                    | 目的                                                                                                                                                  |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 5 | <pre>pattern trunk-to-ext busy tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</pre> <p>例:<br/>Router(config-vm-int)# pattern trunk-to-ext busy 6 FDN * CGN *</p>           | 外部のトランク コールが話中の内線に到達し、コールがボイスメールに転送されるときに、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 デジットパターンの転送を設定します。引数およびキーワードの詳細については、 <a href="#">ステップ 2</a> を参照してください。    |
| 手順 6 | <pre>pattern trunk-to-ext no-answer tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</pre> <p>例:<br/>Router(config-vm-int)# pattern trunk-to-ext no-answer 4 FDN * CGN *</p> | 外部のトランク コールが無応答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 デジットパターンの転送を設定します。引数およびキーワードの詳細については、 <a href="#">ステップ 2</a> を参照してください。 |

## 例

次の設定では、ボイスメール番号が 1101 であり、3001 がメッセージ ボタンを備えた電話機である場合、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ます。このような状況では、3001 は発信者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 に発信し、3006 が応答しなかった場合、Unified SRST ルータは 3001 をボイスメールシステム(1101)に転送し、ボイスメールシステムに DTMF パターン #3006#2 を送信します。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)宛てのものです。このパターンが送信されるには、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 が話中のときに 3001 が 3006 に発信した場合、Unified SRST ルータは 3001 をボイスメールシステム(1101)に転送し、ボイスメールシステムに DTMF パターン #3006#2 を送信します。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)宛てのものです。このパターンが送信されるには、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
```

## メッセージ待機インジケータの設定(Cisco Unified SRST ルータ)

メッセージ待機インジケータ(MWI)リレーメカニズムは、誰かがボイスメールメッセージをリモートボイスメールメッセージシステムに残すと開始されます。MWIリレーは、1つのCisco Unityボイスメールシステムが複数のCisco Unified SRSTルータで共有されているときに必要です。Unified SRSTルータは、SIPのサブスクリイブとMWIのNotify方式を使用します。SIP MWIおよびサブスクリイブとNotify方式については、『[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Unified 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のサブスクリイブとして機能します。

## 制約事項

- MWI は、Unified SRST へのフォールバック中はサポートされません。MWI(電話機の LED インジケータ)は、新しいメッセージの着信時やすべてのメッセージがリッスン済みのときに、そのことを正しく反映しません。WAN リンクが使用可能になり、Unified Communications Manager との接続が再確立されたら、MWI との再同期を推奨します。MWI の動作は、Unified SRST 上の IPv4 と IPv6 のボイスメール サポートでは一貫しています。

## 手順の概要

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**

## 手順の詳細

|      | コマンド                                                                            | 目的                                                          |
|------|---------------------------------------------------------------------------------|-------------------------------------------------------------|
| 手順 1 | <b>call-manager-fallback</b><br><br>例:<br>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。                 |
| 手順 2 | <b>mwi relay</b><br><br>例:<br>Router(config-cm-fallback)# mwi relay             | Unified SRST ルータがリモート Cisco IP Phone に MWI 情報をリレーできるようにします。 |
| 手順 3 | <b>mwi reg-e164</b><br><br>例:<br>Router(config-cm-fallback)# mwi reg-e164       | SIP プロキシまたはレジストラにより、内線番号ではなく E.164 番号を登録します。                |
| 手順 4 | <b>exit</b><br><br>例:<br>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。                 |
| 手順 5 | <b>sip-ua</b><br><br>例:<br>Router(config)# sip-ua                               | SIP ユーザエージェント コンフィギュレーションモードを開始します。                         |

|      | コマンド                                                                                                                                                                                                 | 目的                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 6 | <pre>mwi-server {ipv4:destination-address   dns:host-name} [expires seconds] [port port] [transport {tcp   udp}] [unsolicited]</pre> <p>例:<br/>Router(config-sip-ua)# mwi-server ipv4:10.0.2.254</p> | <p>音声ゲートウェイまたはユーザエージェント上でボイスメールサーバ設定を指定します。SIPベースの MWI サーバの IP アドレスおよびポートは、ボイスメールサーバと同一の LAN 上に存在する必要があります。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。</p> <ul style="list-style-type: none"> <li>• <b>ipv4:destination-address</b>: ボイスメールサーバの IP アドレス。</li> <li>• <b>dns:host-name</b>: ターゲットアドレスに関連付けられた完全なホスト名(たとえば、<b>dns:test.cisco.com</b>)を含める必要があります。</li> <li>• <b>expires seconds</b>: 加入の有効期間(秒単位)。範囲は 1 ~ 999999 です。デフォルトは 3600 です。</li> <li>• <b>port port</b>: 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>• <b>transport</b>: ボイスメールサーバへのトランスポートプロトコル。有効な値は tcp および udp です。デフォルトは UDP です。</li> <li>• <b>unsolicited</b>: メールボックスステータスが変わった場合に、SIP 通知メッセージを音声ゲートウェイまたは UA に送信するようにボイスメールサーバに要求します。MWI サービスに加入するという音声ゲートウェイの要件を削除します。</li> </ul> |
| 手順 7 | <pre>exit</pre> <p>例:<br/>Router(config-sip-ua)# exit</p>                                                                                                                                            | <p>SIP ユーザエージェント コンフィギュレーションモードを終了します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## メッセージ待機インジケータの設定(SRST モードの SIP 電話)

SIP SRST モードで動作している SIP 電話では、**mwi unsolicited** コマンドを使用して、メッセージが Cisco Unity Express (CUE) によって送信されるときにメッセージ待機通知を設定することができます。SIP 電話はその後、ボイスメッセージングシステムから指示されると通知を表示します。メッセージ待機通知を設定するには、次の手順に従います。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **mwi-server {ipv4:destination-address | dns:host-name} [unsolicited]**
5. **exit**

6. `voice register global`
7. `mwi unsolicited`
8. `end`

## 手順の詳細

|      | コマンド                                                                                                                                                                                                                                               | 目的                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 1 | <code>enable</code><br><br>例:<br>Router> enable                                                                                                                                                                                                    | 特権 EXEC モードをイネーブルにします。<br>プロンプトが表示されたら、パスワードを入力します。                                                                                                                                                                                                                                                                                                                                                                         |
| 手順 2 | <code>configure terminal</code><br><br>例:<br>Router# configure terminal                                                                                                                                                                            | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                                                                                                                                                                |
| 手順 3 | <code>sip-ua</code><br><br>例:<br>Router(config)# sip-ua                                                                                                                                                                                            | ユーザ エージェントを設定するために、Session Initiation Protocol (SIP) ユーザ エージェント (ua) コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                                                                                                 |
| 手順 4 | <code>mwi-server {ipv4:destination-address   dns:host-name} [unsolicited]</code><br><br>例:<br>Router(config-sip-ua)# mwi-server ipv4:10.0.2.254 unsolicited<br><br>または<br>Router(config-sip-ua)# mwi-server dns:server.yourcompany.com unsolicited | 音声ゲートウェイまたはユーザ エージェント上でボイスメール サーバ設定を指定します。キーワードと引数は次のとおりです。 <ul style="list-style-type: none"> <li>• <b>ipv4:destination-address</b>: ボイスメール サーバの IP アドレス。</li> <li>• <b>dns:host-name</b>: ターゲット アドレスに関連付けられた完全なホスト名 (たとえば、<b>dns:test.cisco.com</b>) を含める必要があります。</li> <li>• <b>unsolicited</b>: メールボックス ステータスが変更された場合に、SIP 通知メッセージを音声ゲートウェイまたは UA に送信するようにボイスメール サーバに要求します。MWI サービスに加入するという音声ゲートウェイの要件を削除します。</li> </ul> |
| 手順 5 | <code>exit</code><br><br>例:<br>Router(config-sip-ua)# exit                                                                                                                                                                                         | SIP ユーザ エージェント コンフィギュレーション モードを終了します。                                                                                                                                                                                                                                                                                                                                                                                       |
| 手順 6 | <code>voice register global</code><br><br>例:<br>Router(config)# voice register global                                                                                                                                                              | 音声レジスタ グローバル コンフィギュレーション モードを開始して、SIP SRST モードでサポートされるすべての SIP 電話に対してパラメータを設定します。                                                                                                                                                                                                                                                                                                                                           |
| 手順 7 | <code>mwi unsolicited</code><br><br>例:<br>Router(config-register-global)# mwi unsolicited                                                                                                                                                          | MWI 通知を受信するすべての SIP 電話をイネーブルにします。                                                                                                                                                                                                                                                                                                                                                                                           |
| 手順 8 | <code>end</code><br><br>例:<br>Router(config-register-global)# end                                                                                                                                                                                  | 特権 EXEC モードに戻ります。                                                                                                                                                                                                                                                                                                                                                                                                           |

## Unified SRST の設定例

ここでは、次の設定例について説明します。

- ローカル ボイスメール システム (FXO および FXS) の設定: 例 (259 ページ)
- 中央ボイスメール システム (FXO および FXS) の設定: 例 (260 ページ)
- FXO および FXS 経由でのボイスメールへのアクセスの設定: 例 (260 ページ)
- BRI および PRI 経由でのボイスメールへのアクセスの設定: 例 (261 ページ)
- SIP SRST のメッセージ待機インジケータ: 例 (261 ページ)

### ローカル ボイスメール システム (FXO および FXS) の設定: 例

次の例の「Dial-Peer Configuration for Integration of Voicemail with Cisco Unified SRST」セクションは、ローカル ボイスメール システムのレガシー ダイアルピア設定を示します。「Cisco Unified SRST Voicemail Integration Pattern Configuration」セクションは、ユーザのボイスメール システムの設定と互換性がある必要があります。

```
! Dial-Peer Configuration for Integration of voicemail 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 voicemail 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 *
```

## 中央ボイスメール システム (FXO および FXS) の設定:例

次の例の「Dial-Peer Configuration for Integration of voicemail with Cisco Unified SRST in Central Location」セクションは、中央ボイスメール システムのレガシー ダイアルピア設定を示します。「Cisco Unified SRST Voicemail Integration Pattern Configuration」セクションは、ユーザのボイスメール システムの設定と互換性がある必要があります。



(注)

メッセージ待機インジケータ (MWI) の統合は、中央のボイスメール 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 voicemail 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 Voicemail 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 経由でのボイスメールへのアクセスの設定:例

次の例は、Cisco Unified SRST ルータが無応答のコールをボイスメールに転送するように設定する方法を示します。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、音声メールボックス番号は 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 経由でのボイスメールへのアクセスの設定:例

次の例は、Cisco Unified SRST ルータが無応答のコールをボイスメールに転送するように設定する方法を示します。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、音声メールボックス番号は 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
```

## SIP SRST のメッセージ待機インジケータ:例

次の例は、内線 32002宛てにボイスメールがあることを示す NOTIFY メッセージを SRST で受信したことを示します。

```
Received:
NOTIFY sip:32002@10.4.49.65:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP 10.4.49.66:5060;branch=z9hG4bK.D6.7wA19CN6khf305D1MQ~~194
```

```

Max-Forwards: 70
To: <sip:32002@10.4.49.65:5060>
From: <sip:32002@10.4.49.66:5060>;tag=dsd3d29b2f
Call-ID: f0e7ae97-1227@sip:32002@10.4.49.66:5060
CSeq: 1 NOTIFY
Content-Length: 112
Contact: <sip:32002@10.4.49.66:5060>
Content-Type: application/simple-message-summary
Event: message-summary
Messages-Waiting: yes
Message-Account: sip:32002@10.4.49.66
Voice-Message: 1/0 (1/0)
Fax-Message: 0/0 (0/0)

```

## SIP アプリケーションとボイスメールに DTMF リレーを設定する方法

SIP アプリケーション用の DTMF リレーは、2 種類のボイスメールの状況で使用できます。

- [SIP RFC 2833 を使用した DTMF リレー \(262 ページ\)](#)
- [SIP NOTIFY を使用した DTMF リレー \(非標準\) \(264 ページ\)](#)

SIP SRST がコールをボイスメールへ転送する設定については、「[コール処理の設定](#)」セクション (109 ページ) を参照してください。



(注) SIP 電話のメッセージ ボタンに関連する SRST のボイスメール番号は、Cisco Unified Communications Manager (CUCM) によって設定され、SIP SRST では設定できません。SIP SRST のボイスメールシステムに適切なダイヤルピアを設定するには、管理者が CUCM によって設定されたボイスメール番号のセットを把握している必要があります。

## SIP RFC 2833 を使用した DTMF リレー

Cisco Unified SRST システムで使用されているような Cisco Unified Skinny Client Control Protocol (SCCP) 電話は、アウトオブバンド DTMF デジタル表示のみサポートしています。SCCP 電話がデジタル情報をリモート SIP ベースの IVR およびボイスメールアプリケーションに送信できるようにするため、Cisco Unified SRST 3.2 以降のバージョンは、アウトオブバンド SCCP デジタル表示を DTMF リレー向けの SIP 規格である RFC 2833 に変換することができます。この方法は、`dtmf-relay rtp-nte` コマンドを使用して SIP VoIP ダイヤルピアで選択します。

SIP DTMF リレー方式は、次の場合に必要です。

- SIP を使用して、リモートの SIP ベースの IVR または Cisco Unity などのボイスメールアプリケーションに Cisco Unified SRST システムが接続されている。
- SIP を使用して、PSTN を経由してボイスメールまたは IVR アプリケーションに接続するリモートの SIP-PSTN 音声ゲートウェイに Cisco Unified SRST システムが接続されている。



(注) アウトオブバンド DTMF リレー変換を使用する必要があるのは、SCCP 電話だけです。SIP 電話は、RFC 2833 で指定されているように、ネイティブにインバンド DTMF リレーをサポートしています。

RFC 2833 を使用して SIP DTMF リレーを有効にするには、このセクションのコマンドを発信および着信ゲートウェイの両方で使用する必要があります。

## 手順の概要

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**

## 手順の詳細

|      | コマンドまたはアクション                                                                                                                 | 目的                                                                                                                                                                                                                                  |
|------|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 1 | <b>dial-peer voice tag voip</b><br><br>例:<br>Router(config)# dial-peer voice 2 voip                                          | ダイヤルピア コンフィギュレーション モードを開始します。                                                                                                                                                                                                       |
| 手順 2 | <b>dtmf-relay rtp-nte</b><br><br>例:<br>Router(config-dial-peer)# dtmf-relay rtp-nte                                          | Real-Time Transport Protocol (RTP) と Named Telephony Event (NTE) ペイロード タイプを使用して DTMF トーンを転送します。                                                                                                                                     |
| 手順 3 | <b>exit</b><br><br>例:<br>Router(config-dial-peer)# exit                                                                      | ダイヤルピア コンフィギュレーション モードを終了します。                                                                                                                                                                                                       |
| 手順 4 | <b>sip-ua</b><br><br>例:<br>Router(config)# sip-ua                                                                            | SIP ユーザ エージェント コンフィギュレーション モードをイネーブルにします。                                                                                                                                                                                           |
| 手順 5 | <b>notify telephone-event max-duration time</b><br><br>例:<br>Router(config-sip-ua)# notify telephone-event max-duration 2000 | 単一の DTMF イベントに対する 2 つの連続した NOTIFY メッセージ間で許容される最大時間間隔を設定します。<br><br><ul style="list-style-type: none"> <li>• <b>max-duration time</b>: 単一の DTMF イベントに対する連続した NOTIFY メッセージ間の時間間隔 (ミリ秒単位)。範囲は 500 ~ 3000 です。デフォルトは 2000 です。</li> </ul> |
| 手順 6 | <b>exit</b><br><br>例:<br>Router(config-sip-ua)# exit                                                                         | SIP ユーザ エージェント 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のヒント

**show running-config** コマンド出力のダイヤルピア セクションは、ここで引用するように、設定されている場合は DTMF リレー ステータスを表示します。

```
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 を使用した DTMF リレー (非標準)

Cisco Unity Express システムに接続する SIP ネットワークで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 Unified SRST バージョン 3.0 および 3.1 との後方互換性のために必要になることがあります。

### 手順の概要

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**

### 手順の詳細

|      | コマンドまたはアクション                                                                              | 目的                                        |
|------|-------------------------------------------------------------------------------------------|-------------------------------------------|
| 手順 1 | <b>dial-peer voice tag voip</b><br><br>例:<br>Router(config)# dial-peer voice 2 voip       | ダイヤルピア コンフィギュレーション モードを開始します。             |
| 手順 2 | <b>dtmf-relay sip-notify</b><br><br>例:<br>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。     |
| 手順 3 | <b>exit</b><br><br>例:<br>Router(config-dial-peer)# exit                                   | ダイヤルピア コンフィギュレーション モードを終了します。             |
| 手順 4 | <b>sip-ua</b><br><br>例:<br>Router(config)# sip-ua                                         | SIP ユーザ エージェント コンフィギュレーション モードをイネーブルにします。 |

|      | コマンドまたはアクション                                                                                                                      | 目的                                                                                                                                                                                                                                 |
|------|-----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 5 | <pre>notify telephone-event max-duration time</pre> <p>例:<br/>Router(config-sip-ua)# notify telephone-event max-duration 2000</p> | <p>単一の DTMF イベントに対する 2 つの連続した NOTIFY メッセージ間で許容される最大時間間隔を設定します。</p> <ul style="list-style-type: none"> <li>• <b>max-duration time</b>: 単一の DTMF イベントに対する連続した NOTIFY メッセージ間の時間間隔(ミリ秒単位)。範囲は 500 ~ 3000 です。デフォルトは 2000 です。</li> </ul> |
| 手順 6 | <pre>exit</pre> <p>例:<br/>Router(config-sip-ua)# exit</p>                                                                         | <p>SIP ユーザ エージェント コンフィギュレーション モードを終了します。</p>                                                                                                                                                                                       |

## トラブルシューティングのヒント

**show sip-ua status** コマンド出力は、電話イベントに対する連続した NOTIFY メッセージ間の時間間隔を表示します。次の例では、時間間隔が 2000 ms 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
```

## 次の作業

ビデオ パラメータの設定方法については、「[ビデオ パラメータの設定](#)」セクション(267 ページ)を参照してください。

詳細については、「[Cisco Unified SRST 機能の概要](#)」セクション(1 ページ)の章の「[その他の関連資料](#)」セクション(28 ページ)を参照してください。

■ 次の作業



## ビデオパラメータの設定

この章では、Cisco Unified Survivable Remote Site Telephony (SRST) ルータのビデオパラメータの設定方法について説明します。

### 目次

- [ビデオパラメータを設定するための前提条件 \(267 ページ\)](#)
- [ビデオパラメータの設定に関する制約事項 \(268 ページ\)](#)
- [ビデオパラメータの設定に関する情報 \(269 ページ\)](#)
- [Cisco Unified SRST のビデオパラメータの設定方法 \(271 ページ\)](#)
- [Cisco Unified SRST のトラブルシューティング \(280 ページ\)](#)
- [次の作業 \(280 ページ\)](#)

### 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 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 CM 4.0 以降のバージョンを使用していることを確認します。
- Cisco IP Phone が Cisco Unified SRST ルータに登録されていることを確認します。**show ephone registered** コマンドを使用して ephone の登録を確認します。
- Cisco Unified Video Advantage アプリケーションと Cisco Unified IP Phone の間に接続が確立されていることを確認します。

Cisco Unified Video Advantage 1.02 以降のバージョンがインストールされた PC で、Cisco Unified Video Advantage と Cisco Unified IP Phone との間の回線が正常な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。

- Cisco Unified IP Phone に正しいビデオファームウェアがインストールされていることを確認します。**show ephone phone-load** コマンドを使用して、現在の ephone のファームウェアを表示します。次に、ビデオ対応 Cisco Unified IP Phone の最小ファームウェアバージョンを示します。
  - 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 設定を行います。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 設定を行います。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

- この機能では、次のビデオコーデックだけがサポートされます。
  - H.261
  - H.263
  - H.264 (SRST 7.1 から CUVA 用)
- この機能では、次のビデオ形式だけがサポートされます。
  - 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 ビデオについては、**call start slow** を設定する必要があります。
- ビデオ機能は、回線ごとではなく、ephone ごとに設定されます。
- すべてのコール機能制御（ミュートや保留など）は、該当する場合、音声とビデオの両方のコールに適用されます。
- この機能は次の処理をサポートしません。
  - ビデオ機能の動的な追加: ビデオ接続するには、コールセットアップを開始する *前に*、ビデオ機能が提示されている必要があります。
  - 2 つの SCCP エンドポイント間の T-120 データ接続
  - ビデオのセキュリティ
  - SCCP エンドポイントに対する遠端カメラ制御 (FECC)
  - ビデオコーデックの再ネゴシエーション: ネゴシエーション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は、音声だけのコールになります。既存のコールに対してネゴシエートされたコーデックは、新しいコールに対して使用できません。
  - ビデオコーデックのトランスコーディング
- ビデオ対応のエンドポイントが音声専用のエンドポイントに接続すると、音声だけのコールになります。音声だけのコールの間、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関する情報

この機能では、Cisco Unified SRST のビデオパラメータを設定し、Cisco Unified CM とほぼ同等の機能パリティを維持することができます。Cisco Unified SRST がイネーブルであれば、Cisco Unified IP Phone でビデオ機能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 CM で使用したものと同一設定を保持するためです。ただし、Cisco Unified SRST のビデオパラメータを設定するには、call-manager-fallback コンフィギュレーションモードに切り替える必要があります。ビデオの機能セットは、Cisco Unified SRST の音声通話で使用するものと同じです。

ビデオパラメータを設定するには、次の概念を理解しておく必要があります。

- [エンドポイント機能の照合 \(269 ページ\)](#)
- [ビデオコーデック情報の取得 \(269 ページ\)](#)
- [音声専用コールへのフォールバック \(269 ページ\)](#)
- [ビデオエンドポイント用のコールセットアップ \(270 ページ\)](#)
- [RTP ビデオストリームのフロー \(271 ページ\)](#)

## エンドポイント機能の照合

エンドポイント機能は、電話機の登録時に Cisco Unified SRST に保存されます。これらの機能は、コールセットアップのとき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更新できますが、ルータがエンドポイント機能の変更を認識できるのは、コールセットアップのときのみです。電話機にビデオ機能が追加されると、その情報はルータの内部データ構造では更新されますが、次のコールまで有効になりません。ビデオ機能が削除されている場合、コールが終了するまでルータはビデオ機能の調査を続けますが、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、新しいコールがセットアップされたとき、または既存のコールが再開されたときに、毎回実行されます。

## 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、音声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で行われ、ダイヤルピアまたは他の設定を介して H.323 サービスプロバイダー インターフェイス (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、コールセットアップのとき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。

## 音声専用コールへのフォールバック

ビデオ対応のエンドポイントが音声専用のエンドポイントに接続した場合、コールは音声だけの接続になります。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、コールは音声だけになります。

Cisco Unified SRST ルータはコールタイプ フラグを使用して、コールがビデオ対応か、または音声専用かを示します。コールタイプ フラグは、ビデオ機能が一致した場合は `video` に設定され、音声専用の TDM または音声専用の SIP エンドポイントへ接続している場合は `audio-only` に設定されます。



(注) 音声専用の接続中は、ビデオ関連のすべてのメディア メッセージはスキップされます。

## ビデオエンドポイント用のコールセットアップ

SCCP のビデオ エンドポイントを処理するプロセスは、SCCP の音声エンドポイントを処理するプロセスと同じです。ビデオ コールは音声コールの一部となります。音声コール セットアップが失敗すると、ビデオ コールは失敗します。

ビデオのコール セットアップ中に、ビデオメディア パスが必要かどうか判断されます。必要な場合は、対応するビデオメディアパスのセットアップ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 パスのセットアップには、エンドポイントへメッセージを送信してマルチメディア パスをオープンし、マルチメディア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 パスのセットアップには、ビデオ ストリーム用の論理チャンネルをオープンする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 フラグは、エンドポイント機能の照合に基づいたコール セットアップのときに設定されます。コール セットアップの後、コールタイプ フラグを使用して別のビデオメディア パスが必要かどうか判断されます。コール シグナリングは Cisco Unified CME ルータで管理されます。また、メディア ストリームは、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、他のエンドポイントに転送されます。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セットアップ

同じルータ上に存在する 2 つのローカル SCCP エンドポイント間での相互動作では、ビデオ コールのセットアップに、既存のすべての音声コールセットアップが使用されます(メディア セットアップの場合を除きます)。メディア セットアップの場合は、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 および H.323 エンドポイント間でのコールセットアップ

SCCP エンドポイントと H.323 エンドポイント間のコール セットアップは、SCCP エンドポイント間のコール セットアップとほとんど同じです。ただし、ビデオ機能が選択されている場合、ビデオ オープン論理チャンネル(OLC)を送信するために H.323 コール レッグ イベントをポストし、ゲートウェイがビデオ チャンネル用の OLC を生成する点のみが異なります。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 セットアップを開始する前に、ルータ上でビデオをイネーブル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セットアップ

SCCP エンドポイント間で H.323 ネットワークを介してコールをセットアップする場合は、前の 2 つの項で示したプロセスを組み合わせてセットアップします。ルータは、2 つのエンドポイント間のビデオメディアセットアップを制御し、ゲートウェイが OLC を生成できるようにイベントが H.323 コールログにポストされます。

## RTP ビデオストリームのフロー

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では、Real-Time Transport Protocol (RTP) ストリームがフローアラウンドモードになります。SCCP と H.323 のエンドポイント間、または異なる Cisco Unified CME ルータ上の 2 つの SCCP エンドポイント間のビデオストリームでは、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、VoIP コールのエンドポイント間で RTP パケットを直接ストリーミングすることができ、ゲートウェイによる処理は不要です。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、発信コールログ上でコールを再送信します。フローアラウンドモードでは、シグナリングデータのみがゲートウェイに渡され、拡張性とパフォーマンスが改善されます。
- メディアフロースルーモードでは、音声通話と同じビデオメディアパスが含まれます。メディアパケットはゲートウェイを経由するため、互いのネットワークは意識されません。

RTP named-event パケットに関する情報(発信者 ID 番号、IP アドレス、ローカルおよびリモートの両方のエンドポイントのポートなど)を表示するには、以下に出力例を示すように、**show voip rtp connection** コマンドを使用します。

```
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 がイネーブルであれば、Cisco Unified IP Phone でビデオ機能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 CM で使用したのと同じ設定を保持するためです。ただし、Cisco Unified SRST にビデオパラメータを設定することはできません。

Cisco Unified SRST のビデオパラメータの設定では、次の作業を行います。

- [Slow Connect プロシージャの設定 \(272 ページ\)](#)
- [Cisco Unified SRST の確認 \(272 ページ\)](#)
- [Cisco Unified SRST のビデオパラメータの設定 \(279 ページ\)](#)

## Slow Connect プロシージャの設定

Cisco Unified SRST では、ビデオストリームに slow-connect プロシージャが必要です。H.323 エンドポイントで slow connect が必要な理由は、エンドポイント機能の照合が接続メッセージの後に発生するためです。



(注) slow-connect プロシージャについては、「[Configuring Quality of Service for Voice](#)」を参照してください。

slow-connect プロシージャを設定するには、次の手順に従います。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **call start slow**

### 手順の詳細

|      | コマンドまたはアクション                                                                  | 目的                                                             |
|------|-------------------------------------------------------------------------------|----------------------------------------------------------------|
| 手順 1 | <b>enable</b><br><br>例:<br>Router> enable                                     | 特権 EXEC モードをイネーブルにします。<br><br>• プロンプトが表示されたら、パスワードを入力します。      |
| 手順 2 | <b>configure terminal</b><br><br>例:<br>Router# configure terminal             | グローバル コンフィギュレーション モードを開始します。                                   |
| 手順 3 | <b>voice service voip</b><br><br>例:<br>Router(config)# voice service voip     | 音声サービス コンフィギュレーション モードを開始します。                                  |
| 手順 4 | <b>h323</b><br><br>例:<br>Router(config-voi-serv)# h323                        | H.323 音声サービス コンフィギュレーション モードを開始します。                            |
| 手順 5 | <b>call start slow</b><br><br>例:<br>Router(config-serv-h323)# call start slow | H.323 ゲートウェイで、すべての VoIP コールに対して Slow Connect プロシージャを強制的に使用します。 |

## Cisco Unified SRST の確認

Cisco Unified SRST 機能がイネーブルであることを確認し、Cisco Unified IP Phone の設定を確認する手順は、次のとおりです。

## 手順の概要

1. **enable**
2. **show running config**
3. **show call-manager-fallback all**

## 手順の詳細

|      | コマンドまたはアクション                                                                              | 目的                                                                              |
|------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| 手順 1 | <b>enable</b><br><br>例:<br>Router> enable                                                 | 特権 EXEC モードをイネーブルにします。<br><br>• プロンプトが表示されたら、パスワードを入力します。                       |
| 手順 2 | <b>show running config</b><br><br>例:<br>Router# show running config                       | 実行コンフィギュレーションファイル全体の内容を表示します。                                                   |
| 手順 3 | <b>show call-manager-fallback all</b><br><br>例:<br>Router# show call-manager-fallback all | 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設定をフォールバックモードで表示します。 |



(注)

ネットワーク内の Cisco Unified IP Phone の設定ディスプレイを使用して、電話機のデフォルトルータ 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します。

## 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 DN's 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

次の手順を使用して、Cisco Unified SRST システム内のすべてのビデオ対応電話の最大ビットレートを設定します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **call-manager-fallback**
4. ビデオ
5. **maximum bit-rate value**

### 手順の詳細

|      | コマンドまたはアクション                                                                                    | 目的                                                                            |
|------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| 手順 1 | <b>enable</b><br><br>例:<br>Router> enable                                                       | 特権 EXEC モードをイネーブルにします。<br><br>• プロンプトが表示されたら、パスワードを入力します。                     |
| 手順 2 | <b>configure terminal</b><br><br>例:<br>Router# configure terminal                               | グローバル コンフィギュレーション モードを開始します。                                                  |
| 手順 3 | <b>call-manager-fallback</b><br><br>例:<br>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。                                  |
| 手順 4 | <b>video</b><br><br>例:<br>Router(config-call-manager-fallback)# video                           | call-manager-fallback ビデオ コンフィギュレーション モードを開始します。                              |
| 手順 5 | <b>maximum bit-rate value</b><br><br>例:<br>Router(conf-cm-fallback-video)# maximum bit-rate 256 | IP Phone のビデオ最大帯域幅 (Kbps) を設定します。指定できる範囲は 0 ~ 10000000 です。デフォルトは 10000000 です。 |

### 例

次に、Cisco Unified SRST を使用したビデオの設定例を示します。

```
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 のトラブルシューティング

次のコマンドを使用して、Cisco Unified SRST のビデオをトラブルシューティングします。

- SCCP エンドポイントのトラブルシューティングには、次の **debug** コマンドを使用してください。
  - **debug cch323 video**: H.323 SPI 上でビデオ デバッグ トレースをイネーブルにします。
  - **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 メッセージの抽象構文記法 1 (ASN.1) コンテンツを表示します。
  - **debug h245 asn1**: 送信または受信された H.245 メッセージの ASN.1 コンテンツを表示します。
  - **debug voip ccapi inout**: コール制御アプリケーションプログラミング インターフェイス (CPI) を使用して実行パスを表示します。
- ephone のトラブルシューティングには、次の **debug** コマンドを使用してください。
  - **debug ephone message**: Cisco ephone 間のメッセージ トレースをイネーブルにします。
  - **debug ephone register**: ephone に登録のデバッグを設定します。
  - **debug ephone video**: ephone のビデオ トレースを設定します。このビデオ トレースは、ビデオ機能の選択、起動、停止など、コールのさまざまなビデオ状態に関する情報を提供します。
- 基本的なビデオ/ビデオ間のコールを確認するには、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 コールについて、コールの情報を表示します。
  - **show ephone offhook**: 現在オフフックの ephone について、情報およびパケット カウントを表示します。
  - **show voip rtp connections**: RTP named-event パケットの情報 (発信者 ID 番号、IP アドレス、ローカルとリモートの両方のエンドポイントのポートなど) を表示します。

## 次の作業

Cisco Unified SRST のモニタリングおよび維持については、「[Cisco Unified SRST のモニタリングとメンテナンス](#)」セクション(281 ページ)を参照してください。

詳細については、「[Cisco Unified SRST 機能の概要](#)」セクション(1 ページ)の章の「[その他の関連資料](#)」セクション(28 ページ)を参照してください。



## Cisco Unified SRST のモニタリングとメンテナンス

Cisco Unified Survivable Remote Site Telephony (SRST) をモニタおよびメンテナンスするには、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# <code>show call-manager-fallback all</code>            | すべての Cisco Unified IP Phone、音声ポート、および Cisco Unified SRST ルータのダイヤル ピアの詳細設定を表示します。                      |
| Router# <code>show call-manager-fallback dial-peer</code>      | Cisco Unified SRST ルータのダイヤル ピアの出力を表示します。                                                              |
| Router# <code>show call-manager-fallback ephone-dn</code>      | CallManager フォールバック モードの場合の、Cisco Unified IP Phone 宛先番号を表示します。                                        |
| Router# <code>show call-manager-fallback voice-port</code>     | 音声ポートの出力を表示します。                                                                                       |
| Router# <code>show dial-peer voice summary</code>              | すべての音声ダイヤル ピアのサマリーを表示します。                                                                             |
| Router# <code>show ephone phone</code>                         | Cisco Unified IP Phone のステータスを表示します。                                                                  |
| Router# <code>show ephone offhook</code>                       | オフフックのすべての電話について Cisco Unified IP Phone のステータスを表示します。                                                 |
| Router# <code>show ephone registered</code>                    | 現在登録されているすべての電話について Cisco Unified IP Phone のステータスを表示します。                                              |
| Router# <code>show ephone remote</code>                        | ローカル以外のすべての電話 (Address Resolution Protocol (ARP) エントリがない電話) について Cisco Unified IP Phone のステータスを表示します。 |
| Router# <code>show ephone ringing</code>                       | 呼び出し中のすべての電話について Cisco Unified IP Phone のステータスを表示します。                                                 |
| Router# <code>show ephone summary</code>                       | すべての Cisco Unified IP Phone のサマリーを表示します。                                                              |
| Router# <code>show ephone telephone-number phone-number</code> | 特定の電話番号の Unified IP Phone のステータスを表示します。                                                               |
| Router# <code>show ephone unregistered</code>                  | すべての未登録の電話について Unified IP Phone のステータスを表示します。                                                         |
| Router# <code>show ephone-dn tag</code>                        | Unified IP Phone の宛先番号を表示します。                                                                         |
| Router# <code>show ephone-dn summary</code>                    | すべての Cisco Unified IP Phone の宛先番号のサマリーを表示します。                                                         |

| コマンド                                                       | 目的                                             |
|------------------------------------------------------------|------------------------------------------------|
| Router# <code>show ephone-dn loopback</code>               | ループバック モードで Cisco Unified IP Phone 宛先番号を表示します。 |
| Router# <code>show running-config</code>                   | 設定を表示します。                                      |
| Router # <code>show sip-ua status registrar</code>         | SIP レジストラ クライアントを表示します。                        |
| Router# <code>show voice port summary</code>               | すべての音声ポートのサマリーを表示します。                          |
| Router # <code>show voice register all</code>              | すべての SIP SRST 設定、SIP 電話登録、およびダイヤルピアの情報を表示します。  |
| Router # <code>show voice register global</code>           | 音声レジスタ グローバル設定を表示します。                          |
| Router # <code>show voice register pool all</code>         | すべての設定済みの SIP 電話音声レジスタ プールの詳細情報を表示します。         |
| Router # <code>show voice register pool &lt;tag&gt;</code> | 特定の SIP 電話音声レジスタ プールの詳細情報を表示します。               |
| Router # <code>show voice register dial-peers</code>       | SIP-SRST 間で作成されたダイヤルピアを表示します。                  |
| Router # <code>show voice register dn all</code>           | すべての設定済みの音声レジスタ ディレクトリ番号の詳細情報を表示します。           |
| Router # <code>show voice register dn &lt;tag&gt;</code>   | 特定の音声レジスタ ディレクトリ番号の詳細情報を表示します。                 |



# リダイレクトモードを使用する Cisco Unified SIP SRST 機能の設定



(注) この章は、バージョン 3.0 にのみ適用されます。

この章では、リダイレクトモードを使用する Cisco Unified Session Initiation Protocol (SIP) Survivable Remote Site Telephony (SRST) 機能について説明します。

## 目次

- [リダイレクトモードを使用する Cisco Unified SIP SRST 機能の前提条件 \(A-1 ページ\)](#)
- [リダイレクトモードを使用する Cisco Unified SIP SRST 機能の制約事項 \(A-1 ページ\)](#)
- [リダイレクトモードを使用する Cisco Unified SIP SRST 機能に関する情報 \(A-2 ページ\)](#)
- [リダイレクトモードを使用する Cisco Unified SIP SRST 機能の設定方法 \(A-2 ページ\)](#)
- [リダイレクトモードを使用する Cisco Unified SIP SRST 機能の設定例 \(A-6 ページ\)](#)
- [次の作業 \(A-8 ページ\)](#)

## リダイレクトモードを使用する Cisco Unified SIP SRST 機能の前提条件

[「Cisco Unified SRST 機能の概要」セクション \(1-1 ページ\)](#)の「[Cisco Unified SIP SRST を設定するための前提条件](#)」セクション (1-9 ページ)に記載された前提条件をすべて満たしてください。

## リダイレクトモードを使用する Cisco Unified SIP SRST 機能の制約事項

[「Cisco Unified SRST 機能の概要」セクション \(1-1 ページ\)](#)の「[Cisco Unified SIP SRST の設定に関する制約事項](#)」セクション (1-10 ページ)に説明されている制約事項を参照してください。

## リダイレクトモードを使用する Cisco Unified SIP SRST 機能に関する情報

Cisco Unified SIP SRST は、基本レジストラ サービスとリダイレクト サービスを提供することで、外部 SIP プロキシ サーバへのバックアップを行います。これらのサービスは、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 IP Phone によって使用されます。また、Cisco Unified SIP SRST デバイスは、PSTN コールを発信および受信するための PSTN ゲートウェイ アクセスも提供します。

Cisco Unified SIP SRST サービスを最大限活用するためには、ローカル SIP IP Phone がプライマリ SIP プロキシまたはレジストラと Cisco Unified SIP SRST バックアップ レジストラの両方へのデュアル(同時)登録をサポートしている必要があります。Cisco Unified SIP SRST は、次のタイプのコールを処理します。

- 主要なプロキシが使用できない場合、ローカル SIP IP Phone からローカル SIP 電話への発信。
- ローカル SIP IP Phone から発信 PSTN への制限クラス(COR)などの追加サービス。たとえば、発信番号 1 ~ 900 をブロックします。

## リダイレクトモードを使用する Cisco Unified SIP SRST 機能の設定方法

ここでは、次の手順について説明します。

- [Cisco Unified SIP SRST 対応の SIP IP Phone 間のコールをサポートするためのコールリダイレクト拡張機能の設定\(A-2 ページ\)](#) (必須)
- [300 Multiple Choice 送信のサポートの設定\(A-5 ページ\)](#) (必須)

## Cisco Unified SIP SRST 対応の SIP IP Phone 間のコールをサポートするためのコールリダイレクト拡張機能の設定

コールリダイレクト拡張機能は、Cisco IOS 音声ゲートウェイを経由するローカル SIP 電話から別のローカル SIP 電話へのコールをサポートします。この拡張の前は、SIP 電話は、SIP プロキシまたはリダイレクトサーバであるかのように Cisco IOS 音声ゲートウェイを使用して別のローカル SIP 電話への接続を試みて、失敗していました。今では、Cisco IOS 音声ゲートウェイは SIP リダイレクトサーバとして動作できます。音声ゲートウェイは発信者に SIP リダイレクトメッセージで応答するため、コールを発信した SIP 電話は、その接続先へのコールを確立できます。

**redirect ip2ip** (音声サービス) および **redirect ip2ip** (ダイアルピア) コマンドを使用すると、SIP 機能をグローバルに、または特定の着信ダイアルピアに対して有効にできます。Cisco Unified SIP SRST のデフォルトのアプリケーションは、IP-IP リダイレクションをサポートしています。

- [コールをグローバルにサポートするためのコールリダイレクト拡張機能の設定\(A-3 ページ\)](#)
- [特定の VoIP ダイアルピアでコールをサポートするためのコールリダイレクト拡張機能の設定\(A-4 ページ\)](#)



## コールをグローバルにサポートするためのコールリダイレクト拡張機能の設定

すべての VoIP ダイアルピアのグローバル IP-IP コールリダイレクションを有効にするには、音声サービス コンフィギュレーション モードを使用します。



(注)

ダイアルピア コンフィギュレーション モードで IP-IP リダイレクションが設定されている場合、特定のダイアルピアでの設定が、音声サービス コンフィギュレーション モードで入力されたグローバル設定よりも優先されます。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **redirect ip2ip**
5. **end**

### 手順の詳細

|      | コマンドまたはアクション                                                              | 目的                                                                     |
|------|---------------------------------------------------------------------------|------------------------------------------------------------------------|
| 手順 1 | <b>enable</b><br><br>例:<br>Router> enable                                 | 特権 EXEC モードをイネーブルにします。<br><br>• プロンプトが表示されたら、パスワードを入力します。              |
| 手順 2 | <b>configure terminal</b><br><br>例:<br>Router# configure terminal         | グローバル コンフィギュレーション モードを開始します。                                           |
| 手順 3 | <b>voice service voip</b><br><br>例:<br>Router(config)# voice service voip | 音声サービス コンフィギュレーション モードを開始します。                                          |
| 手順 4 | <b>redirect ip2ip</b><br><br>例:<br>Router(config-voi-srv)# redirect ip2ip | Cisco IOS 音声ゲートウェイを使用して、ゲートウェイ上で SIP 電話コールを SIP 電話コールにグローバルにリダイレクトします。 |
| 手順 5 | <b>end</b><br><br>例:<br>Router(config-voi-srv)# end                       | 特権 EXEC モードに戻ります。                                                      |

## 特定の VoIP ダイアル ピアでコールをサポートするためのコールリダイレクト拡張機能の設定

特定の VoIP ダイアル ピアの IP-IP コールリダイレクションを有効にするには、ダイアルピア コンフィギュレーション モードで着信ダイアル ピアに IP-IP コールリダイレクションを設定します。Cisco Unified SIP SRST のデフォルトのアプリケーションは、IP-IP リダイレクションをサポートしています。



(注) ダイアルピア コンフィギュレーション モードで IP-IP リダイレクションが設定されている場合、特定のダイアル ピアでの設定が、音声サービス コンフィギュレーション モードで入力されたグローバル設定よりも優先されます。

### 制約事項

**redirect ip2ip** コマンドは、ゲートウェイの着信ダイアル ピアに設定する必要があります。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **application application-name**
5. **redirect ip2ip**
6. **end**

### 手順の詳細

|      | コマンドまたはアクション                                                                         | 目的                                                                                                                                                                                     |
|------|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 1 | <b>enable</b><br><br>例:<br>Router> enable                                            | 特権 EXEC モードをイネーブルにします。<br><br>• プロンプトが表示されたら、パスワードを入力します。                                                                                                                              |
| 手順 2 | <b>configure terminal</b><br><br>例:<br>Router# configure terminal                    | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                           |
| 手順 3 | <b>dial-peer voice tag voip</b><br><br>例:<br>Router(config)# dial-peer voice 25 voip | ダイアルピア コンフィギュレーション モードを開始します。<br><br>• <b>tag</b> : ダイアル ピアを一意に特定する番号(この番号はローカルでのみ有意義です)。<br><br>• <b>VoIP</b> : これが POTS ネットワーク上で音声カプセル化を使用する VoIP ピアであることを示します。リダイレクトを設定するために使用されます。 |

|      | コマンドまたはアクション                                                                                        | 目的                                                                                                                                                                                                                                                                      |
|------|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 4 | <pre>application application-name</pre> <p>例:<br/>Router(config-dial-peer)# application session</p> | <p>ダイヤル ピアで特定のアプリケーションを有効にします。</p> <ul style="list-style-type: none"> <li>SIP の場合、デフォルトの Tool Command Language (TCL) アプリケーション (Cisco IOS イメージからは <b>session</b> であり、VoIP ダイヤル ピアと POTS ダイヤル ピアの両方に適用できます。</li> <li>アプリケーションは、IP-IP リダイレクションをサポートしている必要があります。</li> </ul> |
| 手順 5 | <pre>redirect ip2ip</pre> <p>例:<br/>Router(config-dial-peer)# redirect ip2ip</p>                    | <p>Cisco IOS 音声ゲートウェイを使用して、特定の VoIP ダイヤル ピアで SIP 電話コールを SIP 電話コールにリダイレクトします。</p>                                                                                                                                                                                        |
| 手順 6 | <pre>end</pre> <p>例:<br/>Router(config-dial-peer)# end</p>                                          | <p>特権 EXEC モードに戻ります。</p>                                                                                                                                                                                                                                                |

## 300 Multiple Choice 送信のサポートの設定

Cisco IOS リリース 12.2(15)ZJ より前では、コールがリダイレクトされた場合、SIP ゲートウェイは 302 Moved Temporarily メッセージを送信していました。ゲートウェイで最初に最長一致したルート (ダイヤルピア接続先パターン) が 302 メッセージの Contact ヘッダーで使用されました。リリース 12.2(15)ZJ では、リダイレクトされる番号に対して接続先への複数のルートが存在する場合 (複数のダイヤルピアが一致する場合)、SIP ゲートウェイは 300 Multiple Choice メッセージを送信し、Contact ヘッダー内に複数のルートが一覧表示されます。

次の設定では、Contact ヘッダー内に表示されるルートの順序をユーザが選択できます。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **redirect contact order [best-match | longest-match]**
6. **end**

## 手順の詳細

|      | コマンドまたはアクション                                                                                                                           | 目的                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 1 | <code>enable</code><br><br>例:<br>Router> enable                                                                                        | 特権 EXEC モードをイネーブルにします。<br><br>• プロンプトが表示されたら、パスワードを入力します。                                                                                                                                                                                       |
| 手順 2 | <code>configure terminal</code><br><br>例:<br>Router# configure terminal                                                                | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                                                                    |
| 手順 3 | <code>voice service voip</code><br><br>例:<br>Router(config)# voice service voip                                                        | 音声サービス コンフィギュレーション モードを開始します。                                                                                                                                                                                                                   |
| 手順 4 | <code>sip</code><br><br>例:<br>Router(config-voi-srv)# sip                                                                              | SIP コンフィギュレーション モードを開始します。                                                                                                                                                                                                                      |
| 手順 5 | <code>redirect contact order [best-match   longest-match]</code><br><br>例:<br>Router(conf-serv-sip)# redirect contact order best-match | 300 Multiple Choice メッセージ内のコンタクトの順序を設定します。キーワードは次のように定義されます。<br><br>• <b>best-match</b> : (任意) 現在のシステム設定を使用してコンタクトの順序を設定します。<br><br>• <b>longest-match</b> : (任意) 接続先パターンの最長一致を最初に使用し、次に 2 番目の最長一致、次に 3 番目の最長一致というようにコンタクトの順序を設定します。これがデフォルトです。 |
| 手順 6 | <code>end</code><br><br>例:<br>Router(config-serv-sip)# end                                                                             | 特権 EXEC モードに戻ります。                                                                                                                                                                                                                               |

## リダイレクトモードを使用する Cisco Unified SIP SRST 機能の設定例

ここでは、次の設定例について説明します。

- [Cisco Unified SIP SRST: 例 \(A-7 ページ\)](#)

## Cisco Unified SIP SRST: 例

ここでは、前のセクションの設定作業に対応する設定例を示します。

```
!
! Sets up the registrar server and enables IP-to-IP redirection and 300
! Multiple Choice support.
!
voice service voip
 redirect ip2ip
 sip
 registrar server expires max 600 min 60
 redirect contact order best-match
!
! Configures the voice-class codec with G.711uLaw and G729 codecs. The codecs are
! applied to the voice register pools.
!
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g729br8
!
! The voice register pools define various pools that are used to match
! incoming REGISTER requests and create corresponding dial peers.
!
voice register pool 1
 id mac 0030.94C2.A22A
 preference 5
 cor incoming call91 1 91011
 translate-outgoing called 1
 proxy 10.2.161.187 preference 1 monitor probe icmp-ping
 alias 1 94... to 91011 preference 8
 voice-class codec 1
!
voice register pool 2
 id ip 192.168.0.3 mask 255.255.255.255
 preference 5
 cor outgoing call95 1 91021
 proxy 10.2.161.187 preference 1
 voice-class codec 1
!
voice register pool 3
 id network 10.2.161.0 mask 255.255.255.0
 number 1 95... preference 1
 preference 5
 cor incoming call95 1 95011
 cor outgoing call95 1 95011
 proxy 10.2.161.187 preference 1 monitor probe icmp-ping
 max registrations 5
 voice-class codec 1
!
voice register pool 4
 id network 10.2.161.0 mask 255.255.255.0
 number 1 94... preference 1
 preference 5
 cor incoming everywhere default
 cor outgoing everywhere default
 proxy 10.2.161.187 preference 1
 max registrations 2
 voice-class codec 1
!
! Configures translation rules to be applied in the voice register pools.
!
translation-rule 1
```

```
Rule 0 94 91
!
! Sets up proxy monitoring.
!
call fallback active
!
dial-peer cor custom
 name 95
 name 94
 name 91
!
! Configures COR values to be applied to the voice register pool.
!
dial-peer cor list call95
 member 95
!
dial-peer cor list call94
 member 94
!
dial-peer cor list call91
 member 91
!
dial-peer cor list everywhere
 member 95
 member 94
 member 91
!
! Configures a voice port and a POTS dial peer for calls to and from the PSTN endpoints.
voice-port 1/0/0
!
dial-peer voice 91500 pots
 corlist incoming call91
 corlist outgoing call91
 destination-pattern 91500
 port 1/0/0
!
```

## 次の作業

詳細については、「[Cisco Unified SRST 機能の概要](#)」セクション(1-1 ページ)の章の「[その他の関連資料](#)」セクション(1-28 ページ)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

この章では、Cisco Unified CM が、フォールバック中および通常の Cisco Unified CM の動作時に、Cisco Unified SRST ゲートウェイをマルチキャスト保留音(MOH)リソースとして使用できるように、Cisco Unified CM および Cisco Unified SRST を設定する方法を説明します。MOH を提供するローカル ゲートウェイを用いた分散 MOH 設計では、WAN 全体に MOH をストリーミングする必要がないため、帯域幅を節約できます。

## このモジュールで紹介する機能情報の入手方法

お使いの Cisco Unified CME のバージョンが、このモジュールで説明されている機能の一部をサポートしていないことがあります。各機能がサポートされているバージョンのリストについては、「[マルチキャスト MOH リソースとしての Cisco Unified SRST の機能情報](#)」セクション (B-41 ページ) を参照してください。

## 目次

- [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 \(B-10 ページ\)](#)
- [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うえでの制約事項 \(B-10 ページ\)](#)
- [Cisco Unified SRST ゲートウェイのマルチキャスト MOH リソースとしての使用に関する情報 \(B-11 ページ\)](#)
- [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 \(B-16 ページ\)](#)
- [Cisco Unified SRST ゲートウェイの設定例 \(B-40 ページ\)](#)
- [次の作業 \(B-41 ページ\)](#)

## 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 CM 3.1.1 以降のバージョンでサポートされています。
- Cisco Unified CM は、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メディア リソース グループ (MRG) とメディア リソース グループ リスト (MRGL) がある。
  - Cisco Unified SRST マルチキャスト MOH リソースが呼び出されたときは常に G.711 が使用されるように、Cisco Unified CM 領域が割り当てられている。
- Cisco Unified SRST ゲートウェイは Cisco IOS リリース 12.2(15)ZJ2 以降のリリースの Cisco Unified SRST 3.0 上で稼働している必要があります。
- Cisco Unified SRST は、H.323、MGCP、SIP などのプロトコルを使用して Cisco Unified CM に登録されている必要があります。
- Cisco Unified SRST を稼働しないブランチの場合、Cisco Unified CM のマルチキャスト MOH パケットは WAN を経由する必要があります。これを実現するには、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」セクションを参照してください。
- 12.3(14)T より前の Cisco IOS では、**ccm-manager fallback-mgcp** コマンドおよび **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 リリースでは、**ccm-manager fallback-mgcp** コマンドおよび **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 は、音声ポートと MGCP ゲートウェイのコール処理の制御を引き継ぐことができます。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うえでの制約事項

- Cisco Unified SRST のマルチキャスト MOH はユニキャスト MOH をサポートしていません。
- ネットワーク全体を通じて、単一の Cisco Unified CM オーディオ ソースのみを使用できます。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 のマルチキャスト MOH は G.711 のみをサポートします。
- H.323 のマルチキャスト MOH は、Cisco Unified Communications Manager 3.3.2 のすべてのバージョンでサポートされているわけではありません。詳細については、[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 リリース 12.2(15)ZJ イメージでは、Cisco Unified SRST マルチキャスト MOH に H.323 モードのサポートは含まれていません。



# Cisco Unified SRST ゲートウェイのマルチキャスト MOH リソースとしての使用に関する情報

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 \(B-11 ページ\)](#)
- [コーデック、ポート番号、および IP アドレス \(B-12 ページ\)](#)
- [マルチキャスト MOH 伝送 \(B-14 ページ\)](#)
- [ライブ フィードからの MOH \(B-14 ページ\)](#)
- [フラッシュ ファイルからの MOH \(B-15 ページ\)](#)

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

Cisco Unified SRST ゲートウェイは、フォールバック中および通常の Cisco Unified CM の動作時に、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。これを実現するには、オーディオ パケットが WAN を経由しないように、Cisco Unified Communications Manager をマルチキャスト MOH 対応に設定する必要があります。これにより、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 に設定されたものと同じマルチキャスト MOH IP アドレスと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、中央の Cisco Unified CM からではなく、ローカル ブランチ ゲートウェイからのマルチキャストである RTP パケットを取得できます。

Cisco Unified SRST ルータが Cisco Unified CM 対応の Cisco IOS 音声ゲートウェイとして使用されている場合に、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 (電話が未登録) のままで、電話と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。この機能は、Cisco Unified SRST ルータがフォールバック モード (電話が Cisco Unified SRST に登録済み) の場合は適用されません。代わりに、マルチキャスト ループバック インターフェイス経由ではなく直接内部パスを介して、PSTN 発信者に MOH が提供されます。

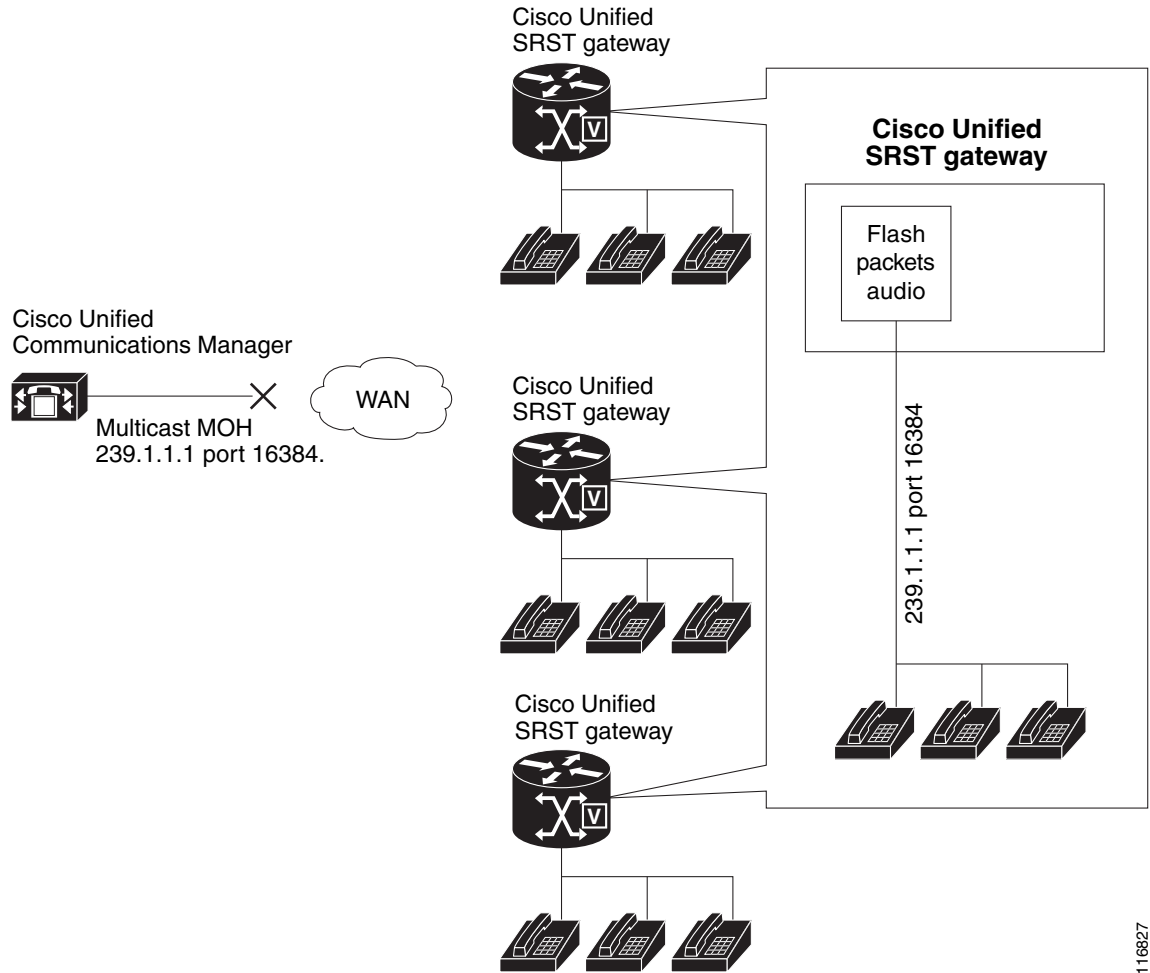
図 1 は、Cisco Unified Communications Manager によって、すべての電話がポート番号 16384 と IP アドレス 239.1.1.1 を介してマルチキャスト MOH を受信するように設定された設定例を示しています。Cisco Unified CM は、マルチキャスト MOH が WAN に到達しないように設定されており、ローカル Cisco Unified SRST ゲートウェイはフラッシュ ファイルからポート番号 16384 と IP アドレス 239.1.1.1 へオーディオ パケットを送信するように設定されています。Cisco Unified CM と IP Phone は、Cisco Unified CM がマルチキャスト MOH の発信元であるかのようにスプーフィングされ動作します。



(注)

セントラル サイトの電話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 1 Cisco Unified SRST フラッシュ メモリからのマルチキャスト MOH



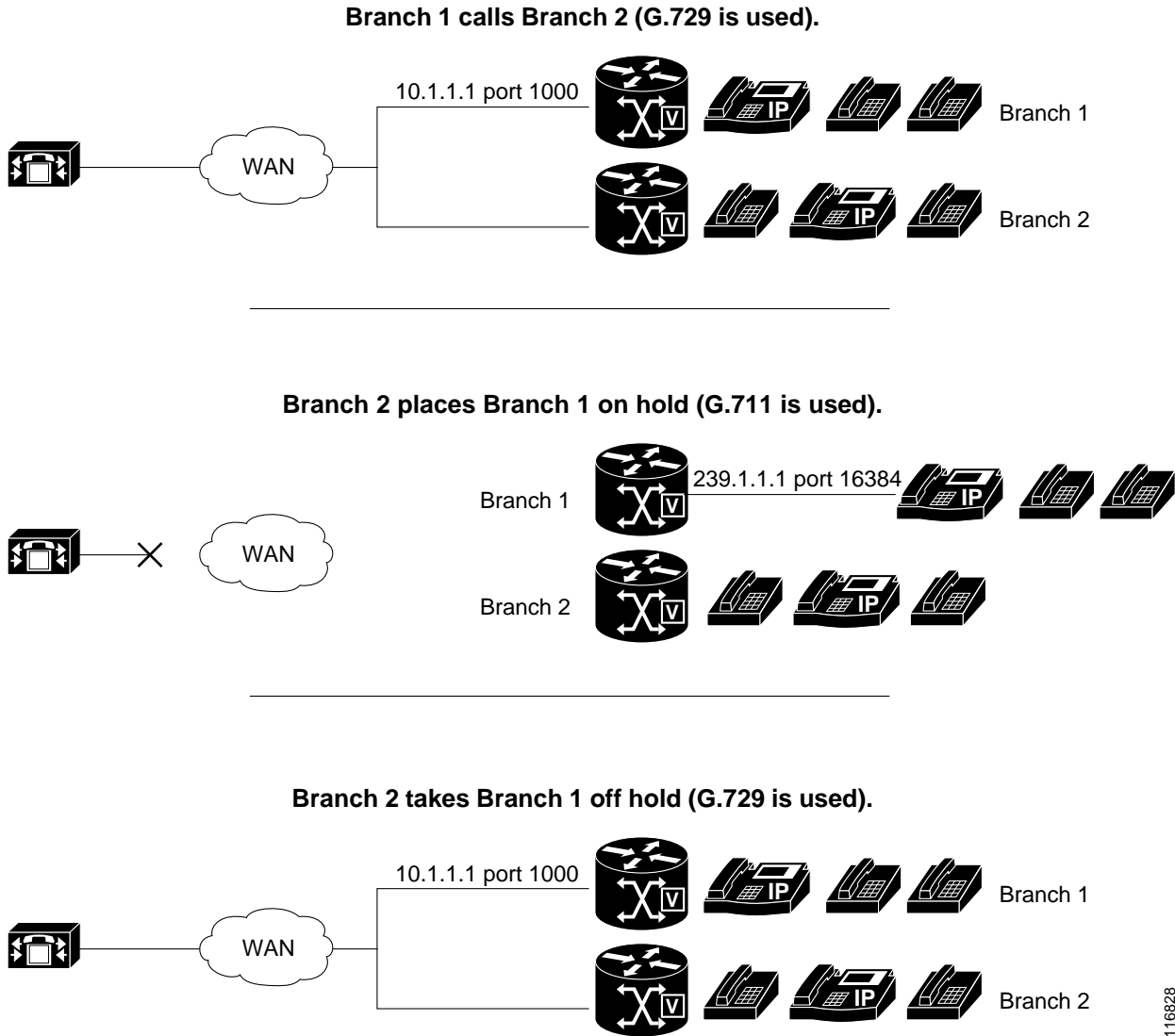
116827

## コーデック、ポート番号、および IP アドレス

Cisco Unified SRST のマルチキャスト MOH は G.711 のみをサポートします。図 2 は、G.711 が中央の Cisco Unified CM と 3 カ所のブランチによって使用されている唯一のコーデックとなっている例を示しています。場合によっては、Cisco Unified CM システムは追加のコーデックを使用できます。たとえば、帯域幅を節約するために、Cisco Unified CM でマルチキャスト MOH 用に G.711 を使用し、電話での会話用に G.729 を使用できます。

図 2 の例に示すように、G.729 が使用されている場合は、電話での会話中に IP アドレス 10.1.1.1 とポート番号 1000 が使用され、コールが保留され G.711 が使用されている場合には IP アドレス 239.1.1.1 とポート番号 16384 が使用されます。

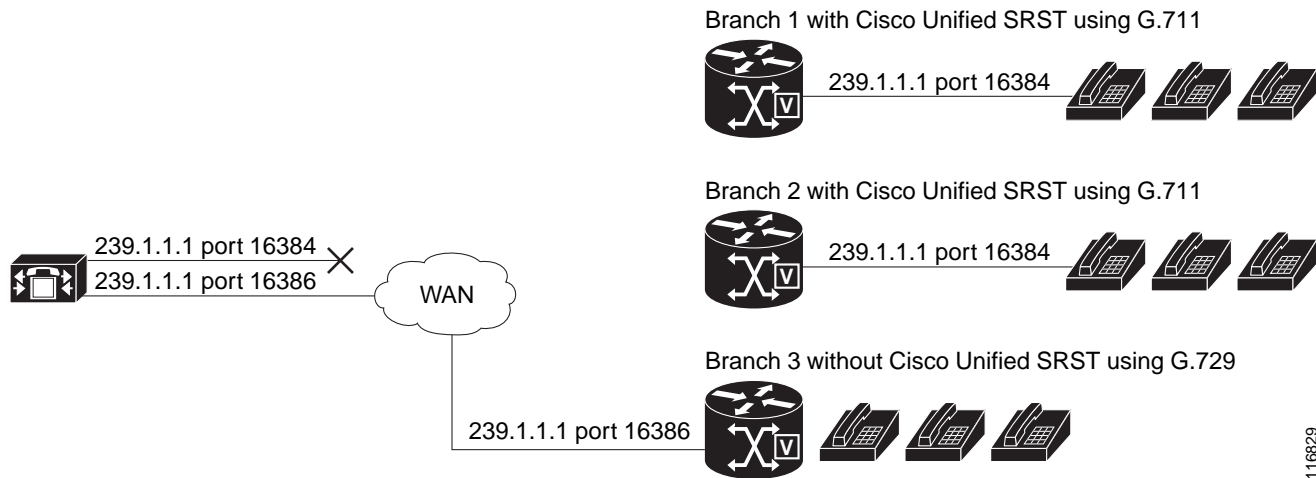
図 2 G.711 および G.729 設定での IP アドレスとポートの使用



116628

図 1 および図 2 は、Cisco Unified SRST マルチキャスト MOH を使用しているすべてのブランチを示しています。図 3 は、一部のゲートウェイに Cisco Unified SRST が設定され、その他のゲートウェイには設定されていない場合を示しています。セントラルサイトとブランチ 3 の電話ユーザが Cisco Unified CM システム内の他の IP Phone によって保留された場合、MOH は Cisco Unified CM から発信されます。ブランチ 1 とブランチ 2 の電話ユーザが Cisco Unified CM システム内の他の電話ユーザによって保留された場合、MOH は Cisco Unified SRST ゲートウェイから発信されます。

図 3 Cisco Unified SRST の MOH ソースおよび MOH を使用する他の Unified SRST IP Phone



2つのパスを通じた MOH オーディオ パケット伝送を有効にするには、一部のブランチが Cisco Unified SRST マルチキャスト MOH を使用し、その他のブランチが Cisco Unified CM マルチキャスト MOH を使用できるように、Cisco Unified CM 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 アドレスのいずれかが設定されている必要があります。

## マルチキャスト MOH 伝送

図 1 などのように、Cisco Unified SRST マルチキャスト MOH がシステム内のすべてのブランチによってサポートされている場合、Cisco Unified Communications Manager は、すべてのマルチキャスト MOH オーディオ パケットが WAN へ到達しないように設定されている必要があります。図 3 に示すように、Cisco Unified SRST ブランチが混在している場合は、一部の Cisco Unified Communications Manager の MOH オーディオ ファイルは WAN に到達する必要があり、それ以外は到達しないようにする必要があります。中央の Cisco Unified Communications Manager からのオーディオ パケットは、Cisco Unified Communications Manager を稼働しているブランチに到達するために WAN を経路する必要があります。Cisco Unified SRST を稼働しているブランチの場合、パケットが WAN に到達しないようにする必要があります。マルチキャスト MOH の詳細については、「Cisco Unified SRST をオーディオ ファイルからのマルチキャスト MOH に対応するように設定」セクション (B-25 ページ) を参照してください。

## ライブ フィードからの MOH

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 へのライブ フィード MOH ストリームを提供します。ライブ フィードからの音楽は、フラッシュ ファイルから読み込まれるのではなく、固定ソースから取得され、連続して MOH プレイアウト バッファにフィードされます。

Cisco Unified SRST は、**moh-live** コマンドによって拡張されます。**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 へのライブ 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 へのマルチキャストである場合もあります。Cisco Unified SRST MOH ライブ フィードの詳細については、「Cisco Unified SRST をライブ フィードからの MOH に対応するように設定」セクション (B-35 ページ) を参照してください。

## フラッシュ ファイルからの MOH

フラッシュ ファイル機能からの MOH マルチキャストは、Cisco Unified Communications がフォールバック中および通常の Cisco Unified Communications のサービス中に、Cisco Unified SRST ブランチ オフィス ルータのフラッシュ メモリ内のファイルからの MOH オーディオ フィードの連続した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 をマルチキャストすると、セントラル オフィスからリモート ブランチに MOH オーディオをストリーミングする必要がなくなるため、WAN 帯域幅を節約できます。

フラッシュ ファイル機能からの MOH マルチキャストは、MOH ライブ フィード機能のバックアップ メカニズムとして稼働できます。フラッシュを使用したライブ フィードのバックアップは、ライブ フィード機能のみを使用したバックアップより推奨される方法です。

Cisco Unified Communications Manager の MOH オーディオ ファイルは WAN に到達する必要がありますが、それ以外は到達しないようにする必要があります。中央の Cisco Unified CM からのオーディオ パケットは、Cisco Unified CM を稼働しているブランチに到達するために WAN を経由する必要があります。Cisco Unified SRST を稼働しているブランチの場合、パケットが WAN に到達しないようにする必要があります。

表 1 に、MOH のオプションの概要を示します。

表 1 保留音(MOH)

| オーディオ ソース          | 説明                                                                                                                                                                                           | 設定方法                                                                                                                                   |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| フラッシュ メモリ          | 外部オーディオ入力は不要です。                                                                                                                                                                              | Cisco Unified SRST をオーディオ ファイルからのマルチキャスト MOH に対応するように設定 (B-25 ページ)                                                                     |
| ライブ フィード           | ローカル IP Phone では、マルチキャスト オーディオ ストリームに最小限の遅延があります。PSTN 発信者の MOH ストリームは、数秒遅延します。ライブ フィード オーディオ入力が失敗すると、保留されている発信者には何も聞こえません。                                                                   | Cisco Unified SRST をライブ フィードからの MOH に対応するように設定 (B-35 ページ)                                                                              |
| ライブ フィードとフラッシュ メモリ | ライブ フィード ストリームは、PSTN とローカル IP Phone 発信者の両方に対して数秒遅延します。フラッシュ MOH は、ライブ フィード MOH のバックアップとして機能します。<br><br>このオプションでは、ライブ フィード入力が見つからないか、失敗した場合に MOH の提供が保証されるため、ライブ フィードを使用する場合は、このオプションが推奨されます。 | Cisco Unified SRST をオーディオ ファイルからのマルチキャスト MOH に対応するように設定 (B-25 ページ)<br>および<br>Cisco Unified SRST をライブ フィードからの MOH に対応するように設定 (B-35 ページ) |

# 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、次のタスクを実行します。

- [Cisco Unified Communications Manager を Cisco Unified SRST マルチキャスト MOH 対応に設定 \(B-16 ページ\)](#)
- [Cisco Unified SRST をオーディオ ファイルからのマルチキャスト MOH に対応するように設定 \(B-25 ページ\)](#)
- [Cisco Unified SRST をライブ フィードからの MOH に対応するように設定 \(B-35 ページ\)](#)

Cisco Unified CM 8.0 以降の場合は、『[Cisco Unified Survivable Remote Site Telephony 8.0 Music On Hold Enhancement](#)』ドキュメントの「[Configuring MOH-groups for Cisco Unified SRST \(fallback\)](#)」セクションを参照してください。

## Cisco Unified Communications Manager を Cisco Unified SRST マルチキャスト MOH 対応に設定

ここでは、Cisco Unified CM を Cisco Unified SRST マルチキャスト MOH 対応に設定するタスク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 \(B-18 ページ\)](#)
- [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 \(B-19 ページ\)](#)
- [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 \(B-21 ページ\)](#)
- [MOH サーバの領域の作成 \(B-23 ページ\)](#)
- [Cisco Unified Communications Manager マルチキャスト MOH の確認 \(B-24 ページ\)](#)

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。これを実現するには、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 CM をソースとするマルチキャスト MOH が実際に WAN とリモートの電話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、設定済みの Cisco Unified CM MOH IP ポートおよびアドレス情報が引き続き Cisco Unified CM によって使用され、MOH (SRST をソースとする MOH) 用にどのマルチキャスト IP アドレスをリッスンするかを電話に通知します。

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。ホップごとに個別に設定することで、Cisco Unified CM マルチキャスト MOH パケットが WAN に到達するのを防止します。それにより、Cisco Unified CM をスプーフィングして、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れらを構成する電話へ送信できます。Cisco Unified CM マルチキャストが Cisco Unified SRST を稼働していないゲートウェイに到達する必要がある場合は、Cisco IOS `ip multicast boundary` コマンドを使用してマルチキャスト パケットの宛先を制御できます。



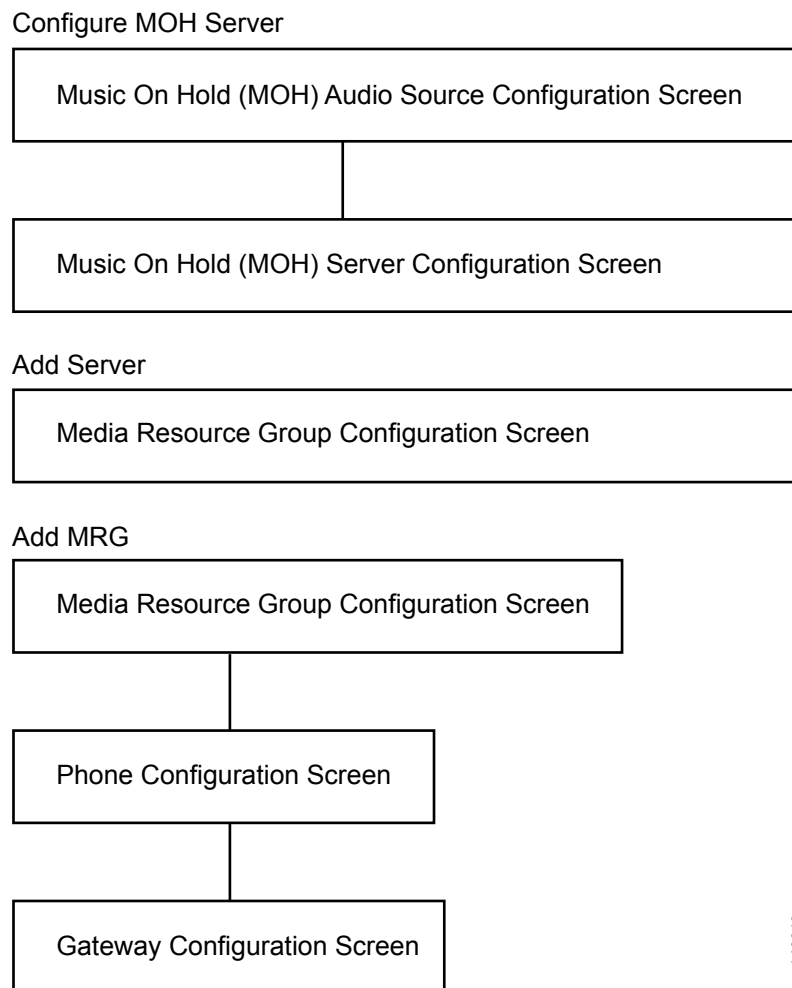
MOH サーバを設定した後、MOH サーバをメディア リソース グループ (MRG) に追加する必要があります。MRG はメディア リソース グループ リスト (MRGL) に追加され、指定された Cisco Unified CM ブランチ ゲートウェイは MRGL を使用するよう設定されます。

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を設定するために、5 つの Cisco Unified CM ウィンドウが使用されます。図 4 は、このプロセスの概要を示しています。

最後の Cisco Unified CM 設定タスクでは、セントラルサイトおよびブランチ オフィス用に MOH G.711 コーデックを使用するように割り当てられた MOH 領域を作成する必要があります。

領域は、領域内および既存の領域間の音声コールとビデオ コールに使用されるコーデックを指定します。領域の詳細については、『Cisco Unified Communications Manager Administration Guide』の「Region Configuration」セクションを参照してください。お使いのバージョンのアドミニストレーション ガイドを見つけるには、Cisco Unified Communications Manager ドキュメント ディレクトリから [メンテナンスおよび運用ガイド (Maintain and Operate Guides)] をクリックして、必要な Cisco Unified Communications Manager バージョンを選択します。

図 4 マルチキャスト MOH を設定するための Unified Communications Manager の画面



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 CM が RTP パケットを送信する際の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か、またはデフォルトのオーディオ ファイルを使用できます。Cisco Unified SRST マルチキャスト MOH の場合、たとえば、500 サイト中 1 サイトが Cisco Unified SRST マルチキャスト MOH を使用しているとしても、1 つのオーディオ ソースしか使用できません。さらに、Cisco Unified SRST マルチキャスト MOH は単一のマルチキャスト IP アドレスとポートにしかオーディオをストリーミングできないため、すべての Cisco Unified Communications Manager システムでユーザ MOH とネットワーク MOH に同じオーディオ ソースを使用する必要があります。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

オーディオ ソースを作成する最も簡単な方法は、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 CM MOH オーディオ ソースを使用するか、新規作成するかに関係なく、MOH オーディオ ソースは [MOH オーディオ ソースの設定 (MOH Audio Source Configuration)] ウィンドウでマルチキャスト用に設定する必要があります。

[MOH オーディオ ソース ファイルのステータス (MOH Audio Source File Status)] セクションに示されているように、MOH オーディオ ソース ファイルが 4 つのコーデック形式に設定されている点に注意してください。複数のコーデックを使用予定の場合は、オーディオ ソース ファイルがそれらに対応していることを確認してください。

MOH オーディオ ソースの作成の詳細については、『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、[メンテナンスおよび運用ガイド (Maintain and Operate Guides)] をクリックして、必要な Cisco Unified CM バージョンを選択します。

MOH オーディオ ソースのマルチキャストと連続再生を有効に設定するには、次の手順を実行します。



(注)

これらの手順は、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。

- 手順 1 MOH オーディオ ソースのマルチキャスト MOH を有効にするには、[サービス (Service)] > [メディア リソース (Media Resources)] > [保留音オーディオ ソース (Music On Hold Audio Source)] を選択し、[MOH オーディオ ソースの設定 (MOH Audio Source Configuration)] ウィンドウを表示します。
- 手順 2 [MOH オーディオ ソース (MOH Audio Sources)] 列にリストされている中から必要なオーディオ ソースをダブルクリックします。
- 手順 3 [MOH オーディオ ソースの設定 (MOH Audio Source Configuration)] ウィンドウで [マルチキャストを許可 (Allow Multicasting)] をオンにします
- 手順 4 [更新 (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

[MOH サーバの設定 (MOH Server Configuration)] ウィンドウの [マルチキャスト オーディオ ソース情報 (Multicast Audio Source Information)] セクションに、基本マルチキャスト IP アドレスとポート番号を入力します。Cisco Unified CM のマルチキャスト MOH および Cisco Unified SRST のマルチキャスト MOH を使用する場合は、「コーデック、ポート番号、および IP アドレス」セクション (B-12 ページ) および「マルチキャスト MOH 伝送」セクション (B-14 ページ) を参照し、2 セットのポート番号と IP アドレスを設定するため、ポートと IP アドレスの増分方法を選択する必要があります。

[マルチキャストの増分をオン (Increment Multicast on)] ラジオ ボタンが [IP アドレス (IP address)] に設定されている場合は、各 MOH オーディオ ソースとコーデックの組み合わせは異なる IP アドレスへ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。これが [ポート番号 (Port Number)] に設定されている場合は、各 MOH オーディオ ソースとコーデックの組み合わせは同じ IP アドレスへ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 2 に、基本 IP アドレス 239.1.1.1 と基本ポート番号 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。この表は、Cisco Unified Communications Manager のオーディオ ソースおよびコーデックと、IP アドレスおよびポート番号の対応も示しています。

表 2 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との違いの例

| オーディオ<br>ソース | コーデック        | IP アドレスの増分によるマルチ<br>キャスト |        | ポート番号の増分によるマルチキャ<br>スト |        |
|--------------|--------------|--------------------------|--------|------------------------|--------|
|              |              | 宛先 IP アドレス               | 接続先ポート | 宛先 IP アド<br>レス         | 接続先ポート |
| 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            | ワイドバンド       | 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            | ワイドバンド       | 239.1.1.8                | 16384  | 239.1.1.1              | 16398  |



(注) 番号の小さい宛先ポート 16384 は最初のマルチキャスト対応オーディオ ソース ID に割り当てられ、後続のポートは後続のマルチキャスト対応オーディオ ソースに割り当てられます。

増分は、コーデックの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、新しい IP アドレスまたはポート番号 (選択された増分に応じて) が新しいコーデック タイプに割り当てられ、使用されます。元のコーデックは IP アドレスとポート番号を保持します。たとえば、表 2 に示すように、基準の IP アドレスとポート番号が G.711  $\mu$ -law コーデック対応の 239.1.1.1 と 16384 であり、コーデックの使用が G.729 に変更された場合 (ポート番号による増分をトリガー)、使用中の IP アドレスとポート番号は 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は 239.1.1.1 と 16384 に戻ります。G.729 が再び使用されると、IP アドレスとポート番号は 239.1.1.1 と 16386 に戻ります。

Cisco Unified SRST マルチキャスト MOH 対応の G.711 オーディオソースを使用する Cisco Unified CM のポート番号と IP アドレスを設定することが重要です。Cisco Unified CM マルチキャスト MOH が、Cisco Unified SRST が存在せず、G.729 などの異なるコーデックを使用しているゲートウェイでも使用されている場合は、追加または増分されたポート番号または 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と必要なコーデックを使用するように確保します。

[MOH サーバの設定 (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 CM MOH サーバは 1 つのオーディオソースのみを使用できます。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。

[最大ホップ数 (Max Hops)] の設定では、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。システム構成に Cisco Unified SRST を稼働しないルータが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 boulder** および **access-list** コマンドを使用します。

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

---

手順 1 Cisco Unified CM のマルチキャスト MOH を有効にします。

- a. [サービス (Service)] > [メディアリソース (Media Resource)] > [保留音サーバ (Music On Hold Server)] を選択します。
- b. [MOH サーバの設定 (MOH Server Configuration)] ウィンドウが表示されます。
- c. [検索 (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 サーバを更新するか、または新しい MOH サーバを作成するかにかかわらず、[この MOH サーバでマルチキャストオーディオソースを有効にする (Enable Multicast Audio Sources on this MOH Server)] をクリックします。

手順 2 基本 IP アドレスとポート番号を設定します。

[MOH サーバの設定 (MOH Server Configuration)] ウィンドウで、[基本マルチキャスト IP アドレス (Base Multicast IP Address)] フィールドに IP アドレスを入力し、[基本マルチキャストポート番号 (Base Multicast Port Number)] フィールドにポート番号を入力します。IP アドレスとポート番号が必要なオーディオソースとコーデックを使用していることを確認します。表 2 を参照してください。

手順 3 Cisco Unified CM がポート番号または 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 アドレスを未変更のままにするには、[MOH サーバの設定 (MOH Server Configuration)] ウィンドウの [マルチキャストの増分をオン (Increment Multicast on)] フィールドで [ポート番号 (Port Number)] を選択します。IP アドレスを増分して、ポート番号を未変更のままにするには、[IP アドレス (IP Address)] を選択します。

- すべてのブランチが Cisco Unified SRST を稼働しており、そのため、MOH に G.711 を使用している場合は、増分は行われず、選択は無関係のため、いずれかの設定を使用します。
- システム構成に Cisco Unified SRST を稼働しないルータが含まれ、異なるコーデックが使用されている場合は、増分方法を選択します。



(注) ブランチに Cisco Unified SRST を稼働しないルータが含まれ、G.711 が使用されている場合は、Cisco Unified SRST を稼働するルータ用と稼働しないルータ用に個別のオーディオソースを設定します。

**手順 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 を稼働する場合は、[MOH サーバの設定 (MOH Server Configuration)] ウィンドウの [オーディオ ソース名 (Audio Source Name)] フィールドの横にある [最大ホップ数 (Max Hops)] フィールドに 1 と入力します。システム構成に Cisco Unified SRST を稼働しないルータが含まれる場合は、[最大ホップ数 (Max Hops)] フィールドに 16 と入力します。

**手順 5** Cisco Unified CM 信号が WAN 経由で Cisco Unified SRST ゲートウェイへ到達しないようにするには、Cisco IOS コマンドを使用します。

すべてのブランチが Cisco Unified SRST を稼働する場合は、この手順は省略します。システム構成に Cisco Unified SRST を稼働しないルータが含まれ、異なるコーデックが使用されている場合は、セントラルサイトのルータのグローバル 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、*port* はポート番号です。

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

管理スコープ境界を設定します。ここで、*access-list-number* は境界によって影響を受けるグループアドレスの範囲を制御するアクセス リストを識別する 1 ~ 99 の番号です。

**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、WAN に到達しないようにする MOH IP アドレスを入力します。通常、これはステップ 2 で入力された基本 IP アドレスです。

設定例を次に示します。

```
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

次のタスクでは、保留中の IP Phone に必要な MOHオーディオ ソースを転送できる MOH サーバを使用するように個々のゲートウェイを設定します。これはメディア リソース グループ (MRG) を作成することで実現されます。MRG は MOH サーバなどのメディア リソースを参照します。次に、MRG はメディア リソース グループ リスト (MRGL) に追加され、MRGL は電話とゲートウェイの設定に追加されます。

MRG は [メディア リソース グループの設定 (Media Resource Group Configuration)] ウィンドウで作成されます。MRGL は [メディア リソース グループ リストの設定 (Media Resource Group List Configuration)] ウィンドウで作成されます。電話は、[電話の設定 (Phone Configuration)] ウィンドウで設定されます。ゲートウェイは、[Gateway Configuration (ゲートウェイの設定)] ウィンドウで設定されます。



(注) H.323 ゲートウェイの [ゲートウェイの設定 (Gateway Configuration)] ウィンドウは、MGCP ゲートウェイの場合と似ています。

MRGL をデバイス プール設定に追加することで、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、[メンテナンスおよび運用ガイド (Maintain and Operate Guides)] をクリックして、必要な Cisco Unified CM バージョンを選択します。

MRG と MRGL を作成して、MOH マルチキャストを有効化し、ゲートウェイを設定するには、次の手順を実行します。

**手順 1** マルチキャスト MOH メディア リソースを伴う MRG を作成します。

- a. [サービス (Service)] > [メディア リソース (Media Resource)] > [メディア リソース グループ (Media Resource Group)] を選択します。
- b. ウィンドウの右上隅で、[新しいメディア リソース グループを追加 (Add a New Media Resource Group)] リンクをクリックします。[メディア リソース グループの設定 (Media Resource Group Configuration)] ウィンドウが表示されます。
- c. [メディア リソース グループ名 (Media Resource Group Name)] フィールドに入力します。
- d. [説明 (Description)] フィールドに入力します。
- e. [使用可能なメディア リソース (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 用に選択できるメディア リソースが一覧表示されます。次のメディア リソース タイプを含めることができます。

- 会議ブリッジ (CFB)
- メディア ターミネーション ポイント (MTP)
- 保留音 (MOH) サーバ
- トランスコーダ (XCODE)
- アナンシエータ (ANN)

マルチキャスト用に設定された保留音サーバは、(MOH) [Multicast] としてラベル付けされます。

- f. 選択されたメディア リソースが [選択されたメディア リソース (Selected Media Resources)] ペインに移動するように、下矢印をクリックします。
- g. [挿入 (Insert)] をクリックします。

- 手順 2** 新しく作成された MRG を含む MRGL を作成します。
- [サービス (Service)] > [メディア リソース (Media Resource)] > [メディア リソース グループ リスト (Media Resource Group List)] を選択します。
  - ウィンドウの右上隅で、[新しいメディア リソース グループ リストを追加 (Add a New Media Resource Group List)] リンクをクリックします。[メディア リソース グループ リストの設定 (Media Resource Group List Configuration)] ウィンドウが表示されます。
  - [メディア リソース グループ リスト名 (Media Resource Group List Name)] フィールドに入力します。
  - [使用可能なメディア リソース グループ (Available Media Resource Groups)] ペインで、作成した MRG を選択します。
  - 下矢印をクリックして、[選択されたメディア リソース グループ (Selected Media Resources Groups)] ペインに MRG を追加します。メディア リソース グループが追加されると、その名前が [選択されたメディア リソース グループ (Selected Media Resources Groups)] ペインに移動します。
  - [挿入 (Insert)] をクリックします。
- 手順 3** 必要な IP Phone に MRGL を追加します。
- [デバイス (Device)] > [電話 (Phone)] を選択して、[電話の検索と一覧表示 (Find and List Phones)] ウィンドウを表示します。
  - [検索 (Find)] をクリックして、電話のリストを表示します。
  - 更新する電話のデバイス名をダブルクリックします。
  - ドロップダウン メニューから必要な MRGL を選択して、[メディア リソース グループ リスト (Media Resource Group List)] フィールドに入力します。
  - [更新 (Update)] をクリックします。
- 手順 4** 必要なゲートウェイに MRGL を追加します。
- [デバイス (Device)] > [ゲートウェイ (Gateway)] を選択して、[ゲートウェイの検索と一覧表示 (Find and List Gateways)] ウィンドウを表示します。
  - [検索 (Find)] をクリックして、ゲートウェイのリストを表示します。
  - 更新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。
  - ゲートウェイが H.323 である場合は、ドロップダウン メニューから必要な MRGL を選択して、[メディア リソース グループ リスト (Media Resource Group List)] フィールドに入力します。
  - [更新 (Update)] をクリックします。

## MOH サーバの領域の作成

MOH サーバが Cisco Unified SRST ゲートウェイ用に G.711 を確実に使用するようにするため、MOH サーバの個別の領域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、「[コーデック、ポート番号、および IP アドレス](#)」セクション (B-12 ページ) を参照してください。領域の詳細については、『[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、[メンテナンスおよび運用ガイド (Maintain and Operate Guides)] をクリックして、必要な Cisco Unified Communications Manager バージョンを選択します。

[領域の設定 (Region Configuration)] ウィンドウを設定します。Cisco Unified CM システムが G.711 のみを使用している場合、MOH 領域に対応するセントラル サイトとその構成要素であるブランチはすべて G.711 に設定する必要があります。Cisco Unified CM システムで、Cisco Unified SRST マルチキャスト MOH を稼働するブランチと稼働しないブランチが組み合わされており、Cisco Unified SRST を稼働しないブランチが Cisco Unified Communications Manager のマルチキャスト MOH 用に異なるコーデックを必要とする場合は、それに応じて設定する必要があります。

「MOH サーバ」領域が G.711 および 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 [領域の設定 (Region Configuration)] ウィンドウは、次のようになります。

- 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 を稼働するように設定されているため、G.711 はブランチ 1 で使用されます。
- ブランチ 2 のゲートウェイは、Cisco Unified SRST を稼働せず、G.729 を使用しているポートと IP アドレスを使用するように設定されているため、G.729 はブランチ 2 で使用されます。
- G.711 はセントラル サイトと MOH サーバ領域用に設定されます。

MOH サーバ用の領域を作成するには、次の手順を実行します。

---

手順 1 MOH サーバ領域を作成します。

- a. [システム (System)] > [領域 (Region)] を選択します。
- b. ウィンドウの右上隅で、[新しい領域を追加 (Add a New Region)] をクリックします。[領域の設定 (Region Configuration)] ウィンドウが表示されます。
- c. [領域名 (Region Name)] フィールドに、新しい領域に割り当てる名前を入力し、[挿入 (Insert)] をクリックします。
- d. 他の領域が作成されている場合は、領域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、新しい領域と既存の領域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って、圧縮のタイプとこれらのコールに割り当てられる最大帯域幅が決まります。
- e. 他の領域に加えて、新しく作成された領域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、新しい領域内で使用するコーデックを選択します。
- f. [更新 (Update)] をクリックします。

手順 2 異なるコーデックが必要な場合は、他の領域を作成します。

---

## 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 を動作させるためには、Cisco Unified CM マルチキャスト MOH の設定が正しく実行されている必要があります。Cisco Unified Communications Manager マルチキャスト MOH の検証は、マルチキャストが有効な WAN を使用する設定と、マルチキャストが無効な WAN を使用する設定では異なります。

Cisco Unified CM マルチキャスト MOH がユニキャストではなく、マルチキャストを介して提供されていることを確認する必要があります。ユニキャスト MOH はデフォルトで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、それが動作していると誤って判断されがちです。



- 
- 手順 1** リモート ゲートウェイで Cisco Unified CM 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。
- マルチキャストが WAN で有効な場合は、Cisco Unified Communications Manager MOH サーバに設定されたホップ数が、オーディオ パケットをリモート サイトに到達させるために十分であることを確認します(「[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](#)」セクション(B-19 ページ)を参照)。その後、リモート ゲートウェイの IP Phone に発信し、コールを保留にして、MOH が聞こえることを確認します。
  - マルチキャストが WAN で有効でない場合は、Cisco Unified Communications Manager MOH サーバと同じサブネット上の IP Phone を保留にして、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、ネットワーク内にマルチキャストルーティング機能は必要ありません。
- 手順 2** Cisco Unified CM 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。
- Microsoft Windows で、[スタート]>[プログラム]>[管理ツール]>[パフォーマンス] を選択します。
  - [パフォーマンス] ウィンドウで、右側のペインの上部にある [+](プラス) アイコンをクリックします。
  - [カウンターの追加] ウィンドウで、[Cisco MOH デバイス (Cisco MOH Device)] を選択します。
  - [パフォーマンス] ウィンドウで、MOHMulticastResourceActive カウンタと MOHUnicastResourceActive カウンタをモニタして、マルチキャストのアクティビティを確認できます。
- 

## Cisco Unified SRST をオーディオ ファイルからのマルチキャスト MOH に対応するように設定



(注) このセクションの手順は、Microsoft Windows を使用して Cisco Unified Communications Manager バージョン 4.3 以前を稼働している場合にのみ実行します。Linux オペレーティング システムでは、Cisco Unified Communications Manager 5.0 以降のバージョンの RTMT (Real-Time Monitoring Tool) を使用して、Cisco Unified CM バージョンの MOH アクティビティをモニタできます。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。

---

オーディオ ファイルからのマルチキャスト MOH に対応するように Cisco Unified SRST を設定するには、次の手順を実行します。

- [Cisco Unified SRST ゲートウェイでのマルチキャスト MOH の有効化\(B-26 ページ\)](#)
- [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\(B-29 ページ\)](#)
- [PSTN への Cisco Unified SRST MOH の確認\(B-30 ページ\)](#)
- [IP Phone への Cisco Unified SRST マルチキャスト MOH の確認\(B-34 ページ\)](#)

## 前提条件

- Cisco Unified SRST ゲートウェイでは Cisco IOS リリース 12.2(15)ZJ2 以降のリリースを実行している必要があります。
- 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 または .au のファイル形式でかまいませんが、A-law または  $\mu$ -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。動作することがわかっている MOH オーディオ ファイル (music-on-hold.au) は、<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key> からダウンロード可能なプログラム .zip ファイルに含まれています。または、music-on-hold.au ファイルを <http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp> からダウンロードして、Cisco Unified SRST ルータのフラッシュ メモリにコピーすることもできます。



(注) SRST ソフトウェアとともにパッケージ化された MOH ファイルは完全に著作権使用料無料です。

- Windows 上で稼働する Cisco Unified CM バージョン 4.3 以前のバージョンでは、SampleAudioSource.ULAW.wav などの MOH ファイルのいずれかを Cisco Unified CM 上の C:\Program Files\Cisco\MOH からコピーして、MOH ファイルをダウンロードします。



(注) コピープロセス中に、4つのファイルが各ルータのフラッシュに自動的に追加されます。ファイルの1つは extension.ULAW.wav で示されるように  $\mu$ -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 のマルチキャスト MOH 設定に含める必要があります。この設定によって、マルチキャスト MOH がゲートウェイの POTS ポートで聞こえるようになります。ループバック インターフェイスを、H.323 または MGCP にバインドする必要はありません。
- ゲートウェイが Cisco Unified SRST 用に使されない場合でも、少なくとも1つの ephone と電話番号 (DN) を設定する必要があります。ephone と電話番号がないと、Cisco Unified SRST マルチキャスト MOH のストリーミングは開始されません。

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

各 Cisco Unified SRST ゲートウェイが、ネットワークからのマルチキャスト MOH パケットをストリーミングするアプリケーションを実行するホストとして機能するように設定されているため、Cisco Unified SRST ゲートウェイにマルチキャスト MOH のルーティングを設定する必要はありません。**multicast moh** コマンドは、Cisco Unified Communications Manager のマルチキャスト 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は、フラッシュ MOH は Cisco Unified SRST **ip source-address** コマンドで設定された IP アドレス経由で送信されます。

### 手順の概要

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**

### 手順の詳細

|      | コマンドまたはアクション                                                                                               | 目的                                                                                                                                                                        |
|------|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 1 | <b>ccm-manager music-on-hold</b><br><br>例:<br>Router(config)# ccm-manager music-on-hold                    | 音声ゲートウェイのマルチキャスト MOH 機能を有効にします。                                                                                                                                           |
| 手順 2 | <b>interface loopback number</b><br><br>例:<br>Router(config)# interface loopback 1                         | インターフェイス タイプを設定して、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。<br><br><ul style="list-style-type: none"> <li>• <i>number</i>: ループバック インターフェイス番号。指定できる範囲は 0 ~ 2147483647 です。</li> </ul> |
| 手順 3 | <b>ip address ip-address mask</b><br><br>例:<br>Router(config-if)# ip address 10.1.1.1 255.255.255.255      | 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。<br><br><ul style="list-style-type: none"> <li>• <i>ip-address</i>: IP アドレス。</li> <li>• <i>mask</i>: 関連付けられている IP サブネットのマスク。</li> </ul>      |
| 手順 4 | <b>exit</b><br><br>例:<br>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。                                                                                                                                           |
| 手順 5 | <b>interface fastethernet slot/port</b><br><br>例:<br>Router(config)# interface fastethernet 0/0            | ( <b>route</b> キーワードが <b>multicast moh</b> コマンドで使用されてい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) 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。                                  |
| 手順 6 | <b>ip address ip-address mask</b><br><br>例:<br>Router(config-if)# ip-address 172.21.51.143 255.255.255.192 | ( <b>route</b> キーワードが <b>multicast moh</b> コマンドで使用されてい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) 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。                                                     |

|       | コマンドまたはアクション                                                                                                                             | 目的                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 7  | <code>exit</code><br><br>例:<br>Router(config-if)# exit                                                                                   | ( <code>route</code> キーワードが <b>multicast moh</b> コマンドで使用されてい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) 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。                                                                                                                                                                                                                                                                                                                    |
| 手順 8  | <code>call-manager-fallback</code><br><br>例:<br>Router(config)# call-manager-fallback                                                    | <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。                                                                                                                                                                                                                                                                                                                                                                                        |
| 手順 9  | <code>ip source-address ip-address [port port]</code><br><br>例:<br>Router(config-cm-fallback)# ip source-address 172.21.51.143 port 2000 | ( <code>route</code> キーワードが <b>multicast moh</b> コマンドで使用されていない場合はオプション。ステップ 13 を参照) ルータが、指定した IP アドレスおよびポート経由で Cisco Unified IP Phone からのメッセージを受信できるようにします。<br><br><ul style="list-style-type: none"> <li>• <code>ip-address</code>: 既存のルータ IP アドレス。通常は、ルータのイーサネット ポートのアドレスのいずれかです。</li> <li>• <code>port port</code>: (任意) Cisco Unified IP Phone からのメッセージを受信するために、ゲートウェイ ルータが接続するポート。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> |
| 手順 10 | <code>max-ephones max-phones</code><br><br>例:<br>Router(config-cm-fallback)# max-ephones 1                                               | ルータがサポートできる Cisco Unified IP Phone の最大数を設定します。<br><br><ul style="list-style-type: none"> <li>• <code>max-phones</code>: ルータがサポートする 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>                                                                                                                                                                                                                                             |
| 手順 11 | <code>max-dn max-directory-number</code><br><br>例:<br>Router(config-cm-fallback)# max-dn 1                                               | ルータがサポートできる仮想音声ポートの最大数を設定します。<br><br><ul style="list-style-type: none"> <li>• <code>max-directory-number</code>: ルータがサポートす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>                                                                                                                                                                                                                                                      |
| 手順 12 | <code>moh filename</code><br><br>例:<br>Router(config-cm-fallback)# moh music-on-hold.au                                                  | MOH ファイルの使用を有効にします。<br><br><ul style="list-style-type: none"> <li>• <code>filename</code>: 音楽ファイルのファイル名。音楽ファイルはフラッシュ メモリ内に存在している必要があります。</li> </ul>                                                                                                                                                                                                                                                                                              |
| 手順 13 | <code>multicasting-enabled</code>                                                                                                        | Cisco Unified CM の管理 GUI の [電話の設定 (Phone Configuration)] ページの [ユーザが保持する MOH オーディオ ソース (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。                                                                                                                                                                                                                                                                                        |

| コマンドまたはアクション                                                                                                                                                                                                                       | 目的                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>手順 14 <code>multicast moh multicast-address port port [route ip-address-list]</code></p> <p>例:<br/> <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> | <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 オフィス内の IP Phone への MOH のマルチキャストを有効にします。</p> <ul style="list-style-type: none"> <li>• <b>multicast-address</b> および <b>port port</b>: マルチキャストする MOH パケットの IP アドレスとポート番号を宣言します。マルチキャスト IP アドレスとポートは、Cisco Unified CM がマルチキャスト MOH 用に使用するように設定されている IP アドレスとポート番号に一致している必要があります。MOH に異なるコーデックを使用する場合、これらは基本 IP アドレスとポートではなく、代わりに増分された IP アドレスまたはポート番号が使用されます。「<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>」セクション (B-18 ページ) 複数のオーディオ ソースが Cisco Unified CM に設定されている場合は、オーディオ ソースの正しい IP アドレスとポート番号が使用されていることを確認します。</li> <li>• <b>route</b>: (任意) IP マルチキャスト パケット用の明示的なルータ インターフェイスのリスト。</li> <li>• <b>ip-address-list</b>: (任意) マルチキャスト MOH 用の、最大 4 つの明示的なルート。デフォルトでは、MOH マルチキャスト ストリームは、<code>ip source-address</code> コマンドで設定したアドレスに対応するインターフェイス上で自動的に出力されます。</li> </ul> |
| <p>手順 15 <code>exit</code></p> <p>例:<br/> <pre>Router(config-cm-fallback)# exit</pre></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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## 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` コマンドを使用して設定されていることを確認するには、次の手順を実行します。

### 手順の概要

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

## 手順の詳細

|      | コマンドまたはアクション                                                                                                                                                                                      | 目的                                                                                                                              |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| 手順 1 | <pre>debug ephone moh</pre> <p>例:</p> <pre>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 !</pre> | 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。          |
| 手順 2 | <pre>show interfaces fastethernet</pre> <p>例:</p> <pre>Router# show interfaces fastethernet 0/0 ! 30 second output rate 86000 bits/sec, 50 packets/sec !</pre>                                    | 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 G.711 ストリームに一致することを確認できます。 <b>show interfaces fastethernet</b> 出力に、50 パケット/秒および 80 kbps 以上として表示されます。 |
| 手順 3 | <pre>show ephone summary</pre> <p>例:</p> <pre>Router# show ephone summary ! File music-on-hold.au type AU Media_Payload_G.711Ulaw64k 160 bytes !</pre>                                            | 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込めたことを確認できます。                                                                 |

## トラブルシューティングのヒント

**show ephone summary** 出力には、ファイルタイプが .au または .wav のいずれかとして表示されます。INVALID が表示された場合は、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 設定コマンドが入力された順序によって引き起こされる場合があります。**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ます。また、再起動によってエラーがクリアされることもあります。

## PSTN への Cisco Unified SRST MOH の確認

Cisco Unified CM の MOH の制御 (WAN リンクがアップ) とマルチキャスト MOH パケットが公衆電話交換網 (PSTN) 経由で転送されていることを確認するには、次の手順を実行します。



(注) この機能は、Cisco Unified SRST ルータがフォールバック モードである場合には適用されません。

## 手順の概要

1. IP Phone の発信者によって保留された場合に、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**

## 手順の詳細

| コマンドまたはアクション                                                                                                                                                                                                                                                                                | 目的                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>手順 1</b> IP Phone の発信者によって保留された場合に、PSTN 発信者に MOH が聞こえることを確認します。</p> <p>Cisco Unified SRST ゲートウェイ IP Phone を使用して PSTN 電話に発信し、PSTN 発信者を保留します。PSTN 発信者には MOH が聞こえるはずですが。</p>                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <p><b>手順 2</b> <b>show ccm-manager music-on-hold</b></p> <p>例:</p> <pre>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</pre> | <p>このコマンドを使用して、Windows および Cisco Unified CM バージョン 4.3 以前のバージョンを使用している場合に、MOH がマルチキャストであることを確認できます。</p> <p><b>show ccm-manager music-on-hold</b> コマンドは、保留されている PSTN 接続に関する情報のみを表示する点に注意してください。保留されている 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しません。次は、<b>show ccm-manager music-on-hold</b> コマンド出力の例です。</p> <p>PSTN 発信者に MOH が聞こえ、<b>show ccm-manager music-on-hold</b> コマンドがアクティブなマルチキャストストリームを表示しない場合、MOH はユニキャストです。</p> <p><a href="#">「Cisco Unified Communications Manager マルチキャスト MOH の確認」セクション (B-24 ページ)</a>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て、これを確認します。</p> |

| コマンドまたはアクション                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 目的                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>手順 3 <b>debug h245 asn</b></p> <p>例:</p> <pre>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 } } }</pre> | <p>このコマンドを使用して、H.323 が使用され、<b>show ccm-manager music-on-hold</b> 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に、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できます。PSTN 発信者を保留すると、Cisco Unified Communications Manager は H.245 <code>closeLogicalChannel</code> を送信し、続いて <code>openLogicalChannel</code> を送信します。Cisco Unified Communications Manager から Cisco Unified SRST ゲートウェイへの最終 <code>openLogicalChannelAck</code> に予期されたマルチキャスト IP アドレスと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 アドレスは EF010101 (239.1.1.1)、ポート番号は 16384 です。</p> |
| <p>手順 4 <b>show call active voice</b></p> <p>例:</p> <pre>Router# show call active voice   include RemoteMedia RemoteMediaIPAddress=239.1.1.1 RemoteMediaPort=16384</pre>                                                                                                                                                                                                                                                                                                                                         | <p>このコマンドを <b>debug h245 asn</b> コマンドと一緒に使用すると、さらに、Cisco Unified Communications Manager と Cisco Unified SRST ゲートウェイとの間の H.323 ハンドシェイクを確認できます。</p> <p>表示された IP アドレスとポート番号は、<b>debug h245 asn</b> コマンドによって表示される IP アドレスとポート番号に一致している必要があります。<code>RemoteMediaIPAddress</code> フィールドに 0.0.0.0 が表示される場合は、おそらく警告 CSCdz00697 が発生しています。詳細については、Cisco <a href="#">Bug Toolkit</a> および「<a href="#">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うえでの制約事項</a>」セクション(B-10 ページ)を参照してください。</p>                                                            |

### トラブルシューティングのヒント

- PSTN 発信者に MOH ではなく保留トーン(TOH)が聞こえる場合は、2 つの問題が考えられます。
  - Cisco Unified CM が MOH の有効化に失敗し、フォールバックとして TOH が使用されている。この場合であることを確認するには、「[Cisco Unified Communications Manager マルチキャスト MOH の確認](#)」セクション(B-24 ページ)を参照してください。
  - Cisco Unified CM で適切な MOH リソースが使用可能でない。MOH リソースが問題であるかどうかを判別するには、**show ccm-manager music-on-hold** コマンドを使用します。



(注) **show ccm-manager music-on-hold** コマンドは、保留されている PSTN 接続に関する情報のみを表示します。保留されている 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しません。

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

```
Current active multicast sessions : 1
Multicast RTP port Packets Call Codec Incoming
Address number in/out id Codec 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、列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)、MRGL がゲートウェイに割り当てられていない、または、MRGL がゲートウェイに割り当てられていてもリソースが不十分であるなどの状態が含まれます。シスコ侵入検知システム(Cisco IDS)のイベントビューアでエラーメッセージを確認します。

- 保留中の POTS 発信者に音が聞こえない場合は、Cisco Unified CM は 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おり、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 ストリームを受け取れていません。

調査するには、**show ccm-manager music-on-hold** コマンドを使用します。

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

```
Current active multicast sessions : 1
Multicast RTP port Packets Call Codec Incoming
Address number in/out id Codec 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 CM 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。典型的なエラーでは、Cisco Unified Communications Manager に適切な MOH リソースが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 CM で有効になっていない(サービス パラメータを確認)、MRGL がゲートウェイに割り当てられていない、または、MRGL がゲートウェイに割り当てられていてもリソースが不十分であるなどの状態が含まれます。IDS のイベントビューアでエラーメッセージを確認します。
- **show ccm-manager music-on-hold** コマンド出力に表示されるマルチキャストアドレスと RTP ポート番号が、**moh multicast** コマンド設定の *multicast-address* および *port* 引数に一致してい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示されていることを確認します。Packets in/out カウンタが増分していることを確認するには、**show ccm-manager music-on-hold** コマンドを繰り返します。

- codec フィールドが、Cisco Unified SRST ゲートウェイのフラッシュ メモリに保存された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 以外の別のコーデック値が表示される場合は、Cisco Unified CM 領域でコーデック設定が間違っていないかどうかを確認します。「[MOH サーバの領域の作成](#)」セクション(B-23 ページ)
- 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ための場所が示されます。1 つのインターフェイスがリストされ、それは **multicast moh** コマンドに含まれるインターフェイスのいずれかであるか、または **ip source-address** コマンドで設定されたデフォルトの IP ソース コマンドである必要があります。  
詳細については、「[Cisco Unified SRST ゲートウェイでのマルチキャスト MOH の有効化](#)」セクション(B-26 ページ)の手順 9 を参照してください。

## IP Phone への Cisco Unified SRST マルチキャスト MOH の確認

Cisco Unified CM 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。

- 
- 手順 1** IP Phone の発信者によって保留された場合に、IP Phone の発信者に MOH が聞こえることを確認します。
- IP Phone を使用して、2 番目の IP Phone に発信し、2 番目の発信者を保留します。2 番目の発信者には MOH が聞こえるはずです。
- 手順 2** MOHMulticastResourceActive カウンタと MOHUnicastResourceActive カウンタを確認します。
- [パフォーマンス] ウィンドウを使用して、Cisco MOH Device パフォーマンス オブジェクトの下の MOHMulticastResourceActive カウンタと MOHUnicastResourceActive カウンタを確認します。「[Cisco Unified Communications Manager マルチキャスト MOH の確認](#)」セクション(B-24 ページ)の手順 2 を参照してください。Cisco Unified SRST マルチキャスト MOH が動作している場合は、マルチキャスト カウンタが増分しています。
- 

## トラブルシューティングのヒント

MOH が聞こえず、Cisco Unified SRST MOH シグナリングがマルチキャストされている場合は、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、IP Phone が保留されていない場合でも、常にマルチキャスト RTP パケットが検出されなければなりません。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 が保留されており、Internet Group Management Protocol (IGMP) Join が最も近いルータに送信された場合のみ、マルチキャスト RTP パケットが検出されます。



## Cisco Unified SRST をライブ フィードからの MOH に対応するように設定

ここでは、Cisco Unified SRST MOH ライブ フィードの設定タスクについて説明します。

- [前提条件 \(B-36 ページ\)](#)
- [制約事項 \(B-36 ページ\)](#)
- [Cisco Unified SRST ゲートウェイの音声ポートの設定 \(B-36 ページ\)](#)
- [Cisco Unified SRST ゲートウェイでの電話番号の設定 \(B-37 ページ\)](#)
- [MOH フィードの確立 \(B-38 ページ\)](#)
- [Cisco Unified SRST MOH ライブ フィードの確認 \(B-40 ページ\)](#)

ライブ フィードからの MOH を設定するには、コール用の音声ポートとダイヤル ピアを確立し、その後、「ダミー」の電話または電話番号を作成します。ダミー番号は、コールの発信と受信が可能で、その番号は物理的な電話には割り当てられていません。これは、MOH フィードを確立するために MOH システムが自動ダイヤルする番号です。

**moh-live** コマンドは、**max-dn** コマンドによって作成された仮想音声ポートのプールから仮想音声ポートの 1 つを割り当てます。仮想音声ポートはダミー番号、つまり、**moh-live** コマンドで指定された電話番号へコールを発信します。MOH コールから取得したオーディオストリームが、保留音オーディオストリームを提供します。

ライブ フィード MOH のインターフェイスには最低限の数の外部コンポーネントが必要となるため、ライブ フィード MOH のインターフェイスはアナログ E&M ポートにすることを推奨します。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 インターフェイス カード (WIC) には、外部オーディオ ソースと正しく電氣的に分離するためのオーディオ変圧器が内蔵されています (E&M ポート上のオーディオ接続に、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 シグナリングをディセーブルにします。E&M ポート上のデジタル シグナル プロセッサ (DSP) により、G.711 オーディオ パケット ストリームが生成されます。

Cisco IOS リリース 12.4(15)T 以降では、音声ポート上で **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 ソースを直接 FXO に接続できます。それ以外の場合には、サードパーティの外部アダプタを通してポートを接続して、バッテリー提供を行う必要があります。外部アダプタは、通常の電話会社 (telco) バッテリ電圧を正しい極性で、FXO ポートのチップアンドリングリードに提供する必要があります。また、外部オーディオ ソースと FXO ポートのチップアンドリングリードの間を、トランスで分離する必要があります。

フラッシュ ファイルから音楽を読み取るのではなく、ライブ フィードからの音楽を MOH プレイアウト バッファに連続的に供給するので、通常は 2 秒の遅延が発生します。MOH 用に設定された電話番号によって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 秒ごとに試行 (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た場合、フラッシュ メモリ ソースが自動的に有効化されます。

ライブ フィード MOH 接続が、Cisco Unified SRST MOH システムによって作成されたか、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作成された、自動的に接続される音声コールとして確立されます。MOH コールは、PSTN から、または PSTN に対して実行するか、または音声アクティビティ検出 (VAD) がディセーブルの VoIP を介して実行できます。設定時に **moh-live** コマンドで **out-call** キーワードを使用した場合を除いて、コールは着信コールであると見なされます。

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 ファイルで使用可能なすべてのオーディオ ストリームは利用されなくなります。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、電話番号に発信してオーディオ ストリームを Cisco Unified SRST ルータに配信する外部 H.323 ベースのサーバ デバイスがあります。

## 前提条件

「Cisco Unified SRST をオーディオ ファイルからのマルチキャスト MOH に対応するように設定」セクション(B-25 ページ)に説明されているとおり、マルチキャスト MOH に対応した Cisco Unified SRST は MOH ライブ フィード設定では必要ありません。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

- FXO ポートにバッテリー供給を行うサードパーティの外部アダプタが搭載されている場合は、そのポートをライブ フィード用に使用できます。
- FXS ポートはライブ フィードには使用できません。
- VoIP からのライブ フィードでは、VAD がディセーブルになっていること。
- MOH は、PSTN コールと VoIP G.711 コールに提供されます。Cisco Unified SRST の一部のバージョンは、MOH をローカル電話に提供します。ローカル IP Phone 用に MOH をサポートしていない Cisco Unified SRST では、保留された発信者には、繰り返し保留トーンが聞こえ、まだ接続されていることを確認できます。
- CPU 使用率が高まり短時間のスパイクによって引き起こされる状況がネットワーク内で発生することがあります。CPU 使用率の短時間のスパイクは、TDM (FXO、PRI、S) インターフェイスを介して接続されている双方に聞こえる MOH の音質に一時的に影響する可能性があります。

## Cisco Unified SRST ゲートウェイの音声ポートの設定

ライブ フィードからの MOH を有効化し、物理的な音声ポートを設定して接続するには、次の手順を実行します。

### 手順の概要

1. **voice-port port**
2. **input gain decibels**
3. **auto-cut-through** (E&M 専用)
4. **operation 4-wire** (E&M 専用)
5. **signal immediate** (E&M 専用)
6. **no shutdown**
7. **exit**

## 手順の詳細

|      | コマンドまたはアクション                                                                          | 目的                                                                                                                                                                                  |
|------|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 1 | <code>voice-port port</code><br><br>例:<br>Router(config)# voice-port 1/1/0            | 音声ポート コンフィギュレーション モードを開始し、物理的な音声ポートを設定します。お使いのルータの <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。 |
| 手順 2 | <code>input gain decibels</code><br><br>例:<br>Router(config-voice-port)# input gain 0 | インターフェイスの受信者側で挿入されるゲインの量をデシベル単位で指定します。有効な値は、-6 ~ 14 の整数です。                                                                                                                          |
| 手順 3 | <code>auto-cut-through</code><br><br>例:<br>Router(config-voiceport)# auto-cut-through | (E&M ポートのみ)PBX が M リード応答を提供しない場合に、コールの完了をイネーブルにします。MOH では、このコマンドを E&M ポートで使用する必要があります。                                                                                              |
| 手順 4 | <code>operation 4-wire</code><br><br>例:<br>Router(config-voiceport)# operation 4-wire | (E&M ポートのみ)4 線ケーブル配線方式を選択します。MOH では、E&M ポートに対して、このコマンドで 4 線動作を指定する必要があります。                                                                                                          |
| 手順 5 | <code>signal immediate</code><br><br>例:<br>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は、E リードでオフフックにすることで回線を確認し、アドレス情報を DTMF の桁として送信するよう発信側に指示します。                                                                                      |
| 手順 6 | <code>no shutdown</code><br><br>例:<br>Router(config-voiceport)# no shutdown           | 音声ポートをアクティブにします。                                                                                                                                                                    |
| 手順 7 | <code>exit</code><br><br>例:<br>Router(config-voiceport)# exit                         | 音声ポート コンフィギュレーション モードを終了します。                                                                                                                                                        |

## Cisco Unified SRST ゲートウェイでの電話番号の設定

音声ポートを設定した後、ダイヤルピアを作成し、**destination-pattern** コマンドを使用して音声ポートに電話番号を指定します。電話番号は、システムが MOH にアクセスするために使用する番号です。

### 手順の概要

1. `dial-peer voice tag pots`
2. `destination-pattern string`
3. `port port`
4. `exit`

## 手順の詳細

|      | コマンドまたはアクション                                                                                            | 目的                                                                                  |
|------|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| 手順 1 | <code>dial-peer voice tag pots</code><br><br>例:<br>Router(config)# dial-peer voice 7777 pots            | ダイヤルピア コンフィギュレーション モードを開始します。                                                       |
| 手順 2 | <code>destination-pattern string</code><br><br>例:<br>Router(config-dial-peer)# destination-pattern 7777 | システムが MOH を作成するために使用する電話番号を指定します。このコマンドは、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。 |
| 手順 3 | <code>port port</code><br><br>例:<br>Router(config-dial-peer)# port 1/1/0                                | 「Cisco Unified SRST ゲートウェイの音声ポートの設定」セクション(B-36 ページ)で指定した音声ポートにダイヤルピアを関連付けます。        |
| 手順 4 | <code>exit</code><br><br>例:<br>Router(config-dial-peer)# exit                                           | ダイヤルピア 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

MOH フィードを確立し、CD プレーヤーなどの音楽ソースに接続して、電話番号を自動ダイヤルするには、次の手順を実行します。

## 手順の概要

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`

## 手順の詳細

|      | コマンドまたはアクション                                                                               | 目的                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 手順 1 | <code>call-manager-fallback</code><br><br>例:<br>Router(config)# call-manager-fallback      | <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。                                                                                                                                   |
| 手順 2 | <code>max-dn max-directory-number</code><br><br>例:<br>Router(config-cm-fallback)# max-dn 1 | ルータがサポートできる仮想音声ポートの最大数を設定します。<br><br><ul style="list-style-type: none"> <li>• <code>max-directory-number</code>: ルータがサポートす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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>手順 3 <code>multicast moh multicast-address port port</code><br/> <code>[route ip-address-list]</code></p> <p>例:<br/> Router(config-cm-fallback)# multicast moh<br/> 239.1.1.1 port 16386 route 239.1.1.2 239.1.1.3<br/> 239.1.1.4 239.1.1.5</p> | <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 オフィス内の IP Phone への MOH のマルチキャストを有効にします。</p> <p>(注) ライブ フィード MOH をマルチキャスト Cisco Unified CM モードへ送るには、このコマンドを使用する必要があります。ストリクト SRST モードである必要はありません。</p> <ul style="list-style-type: none"> <li>• <i>multicast-address</i> および <b>port port</b>: マルチキャストする MOH パケットの IP アドレスとポート番号を宣言します。マルチキャスト IP アドレスとポートは、Cisco Unified Communications Manager がマルチキャスト MOH 用に使用するように設定されている IP アドレスとポート番号に一致している必要があります。MOH に異なるコーデックを使用する場合、これらは基本 IP アドレスとポートではなく、増分された IP アドレスまたはポート番号が使用されます。「<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>」セクション(B-18 ページ)複数のオーディオソースが Cisco Unified CM に設定されている場合は、オーディオソースの正しい IP アドレスとポート番号が使用されていることを確認します。</li> <li>• <b>route ip-address-list</b>: (任意) フラッシュ MOH パケットの転送元となることができる IP アドレスを宣言します。最大 4 つの IP アドレス エントリが許可されます。<b>route</b> 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 用に設定された <b>ip source-address</b> コマンド値を使用します。</li> </ul> |
| <p>手順 4 <code>moh-live dn-number calling-number out-call outcall-number</code></p> <p>例:<br/> Router(config-cm-fallback)# moh-live dn-number 3333 out-call 7777</p>                                                                                | <p>この電話番号が発信コールに使用されるように、つまり、MOH ストリームのソースになるように指定します。</p> <ul style="list-style-type: none"> <li>• <b>dn-number calling-number</b>: 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桁です。</li> <li>• <b>out-call outcall-number</b>: ルータが MOH に使用されるライブ フィードを呼び出していることを示し、発信される番号を指定します。<i>outcall-number</i> 引数は、通常、E&amp;M ポートの電話番号を表す一連の桁です。</li> </ul> <p><b>outcall</b> キーワードは、「<a href="#">Cisco Unified SRST ゲートウェイの音声ポートの設定</a>」セクション(B-36 ページ)で指定されたローカルルータ音声ポートへの接続を確立します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <p>手順 5 <code>exit</code></p> <p>例:<br/> 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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## 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、`debug ephone moh` コマンドおよび「[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](#)」セクション(B-29 ページ)で説明されている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、次の Cisco Unified SRST ゲートウェイの設定例を示します。

- [2つの IP アドレスにルーティングされる MOH:例\(B-40 ページ\)](#)
- [MOH ライブ フィード:例\(B-40 ページ\)](#)

### 2つの IP アドレスにルーティングされる MOH:例

次の例は、Cisco Unified CM マルチキャスト MOH の IP アドレス 239.1.1.1 とポート番号 16384 を宣言し、`music-on-hold.au` オーディオ ファイル パッケージを IP アドレス 10.1.1.1 および 172.21.51.143 が設定されたインターフェースからストリーミングします。

```
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)

マルチキャスト IP アドレスとポートは、Cisco Unified CM がマルチキャスト MOH 用に使用するよう設定されている IP アドレスとポート番号に一致する必要があります。MOH に異なるコーデックを使用する場合、これらは基本 IP アドレスとポートではなく、増分された IP アドレスまたはポート番号が使用されます。「[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](#)」セクション(B-18 ページ)を参照してください。複数のオーディオソースが Cisco Unified CM に設定されている場合は、オーディオソースの正しい IP アドレスとポート番号が使用されていることを確認します。

### MOH ライブ フィード:例

次の例は、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た E&M ポートを参照し、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たアウトコール番号に一致している点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
!
!
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 の機能情報

表 3 は、マルチキャスト MOH リソース機能としての Cisco Unified SRST への拡張機能をバージョン別に一覧表示しています。

ハードウェアとソフトウェアの互換性を確認するには、次の URL で Cisco Unified CM の [互換性情報 (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)

また、次の URL で Cisco Unified CM のドキュメント ロードマップも参照してください。

[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)

プラットフォームのサポート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検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator では、どの Cisco IOS ソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートしているかを確認できます。Cisco Feature Navigator にアクセスするには、<http://www.cisco.com/go/cfn> に移動します。Cisco.com のアカウントは必要ありません。



(注) 表 3 には、特定の機能に対するサポートを導入した Cisco Unified SRST のバージョンが示されています。特に明記されていない限り、Cisco Unified SRST ソフトウェアの後続のバージョンでもこの機能をサポートします。

表 3 マルチキャスト MOH リソースとしての Cisco Unified SRST の機能情報

| 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。 |

## 次の作業

詳細については、「Cisco Unified SRST 機能の概要」セクション (1-1 ページ) の章の「その他の関連資料」セクション (1-28 ページ) を参照してください。

