



## SRTP に対する SIP サポートの設定

---

ここでは、Secure Real-time Transport Protocol (SRTP) の Session Initiation Protocol (SIP) サポートの設定に関する情報を記載します。SRTP は、Real-time Transport Protocol (RTP; リアルタイムトランスポート プロトコル) Audio/Video Profile (AVP) を拡張したものであり、認証、暗号化、および SIP エンドポイント間のメディア パケットの統合を提供する、RTP と Real-Time Control Protocol (RTCP) パケットの統合を確保します。

SRTP に対する SIP サポートは、Cisco IOS リリース 12.4(15)T で導入されました。これ以降のリリースでは、Secure RTP コールの処理を Cisco IOS 音声ゲートウェイ上でグローバルに、またはダイヤルピアごとに設定できます。また、ゲートウェイ (またはダイヤルピア) を (ノンセキュア) RTP にフォールバックするように設定することも、エンドポイントが SRTP をサポートしていない場合は、コールを拒否する (失敗させる) ように設定することもできます。

SRTP と RTP エンドポイント間のネゴシエーションを許可するオプションが、Cisco Unified Communications Manager を搭載した Cisco IOS 音声ゲートウェイにおける STRP に対する SIP サポートの相互運用性として、Cisco IOS リリース 12.4(20)T 以降で追加されました。Cisco IOS リリース 12.4(22)T 以降では、SRTP に対する SIP サポートを Cisco Unified Border Elements (Cisco UBE) にも設定できるようになりました。

## 機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の一部がサポートされていない場合があります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「[SRTP に対する SIP サポート設定に関する機能情報](#)」(P.16) を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスしてください。Cisco.com のアカウントは必要ありません。

## この章の構成

- 「SRTP に対する SIP サポート設定の前提条件」 (P.2)
- 「SRTP に対する SIP サポート設定の制限事項」 (P.2)
- 「SRTP に対する SIP サポート設定について」 (P.3)
- 「SRTP に対する SIP サポートの設定方法」 (P.9)
- 「ダイヤルピアにおける SRTP および SRTP フォールバックの設定」 (P.12)
- 「その他の参考資料」 (P.14)
- 「SRTP に対する SIP サポート設定に関する機能情報」 (P.16)
- 「用語集」 (P.18)

## SRTP に対する SIP サポート設定の前提条件

- 作業 IP ネットワークの確立と VoIP の設定。



(注) VoIP の設定の詳細については、『*Enhancements to the Session Initiation Protocol for VoIP on Cisco Access Platforms*』 ([http://www.cisco.com/en/US/docs/ios/12\\_2t/12\\_2t11/feature/guide/ftsipgv1.html](http://www.cisco.com/en/US/docs/ios/12_2t/12_2t11/feature/guide/ftsipgv1.html)) を参照してください。

- ゲートウェイで SIP の音声機能が設定されていることを確認。
- 使用中のシスコ ルータに十分なメモリが搭載されていることを確認。
- 必要に応じて、ルータでグリニッジ標準時 (GMT) を使用できるように設定。SIP のすべての時間は GMT で送信されるため、GTM の設定が必要です。SIP INVITE メッセージも GMT で送信されます。ただし、ルータはデフォルトで Coordinated Universal Time (UTC; 協定世界時) を使用するよう設定されています。ルータで GMT を使用するよう設定するには、グローバル コンフィギュレーション モードで **clock timezone** コマンドを発行し、GMT を指定します。

## SRTP に対する SIP サポート設定の制限事項

- SIP ゲートウェイは、「*Configuring SIP QoS Features*」モジュールの「*Enhanced Codec Support for SIP Using Dynamic Payloads*」セクション ([http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip\\_cg-qos.html](http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-qos.html)) に掲載されている「SIP Codec Support by Platform and Cisco IOS Release」というタイトルの表にリストされていないコーデックはサポートしません。
- SIP のすべての時間は GMT で送信されるため、GTM の設定が必要です。

# SRTP に対する SIP サポート設定について

SRTP に対する SIP サポート機能は、2 つの SIP エンドポイント間のメディア フローをセキュリティ 保護するため、暗号化を使用します。Cisco IOS 音声ゲートウェイおよび Cisco Unified Border Elements は、ユーザ認証に Digest 方式を使用し、シグナリングの認証と暗号化には、通常、Transport Layer Security (TLS) を使用します。



(注) より高い柔軟性を提供するため、Cisco IOS リリース 12.4(22)T 以降のリリースでは、TLS シグナリング暗号化は、使用されなくなりました。Secure SIP (SIPS) は、現在でも TLS の確立と判別に使用されていますが、TLS は、現在では SRTP の要件ではありません。つまり、SIP のみで (SIPS を使用せずに) 確立されたコールは、現在も TLS シグナリング暗号化を使用せずに SRTP と正常にネゴシエートすることができるということです。これは、IP セキュリティなどの異なるプロトコルを使用しても暗号化を設定できるということにもなります。

ただし、シスコでは TLS シグナリング暗号化を使用せずに STRP に対する SIP サポートを設定することを推奨しません。TLS を使用しないことにより、メディアの暗号化 (SRTP) を強制する意図が損なわれるためです。

TLS を使用する場合は、Session Description Protocol (SDP) の暗号アトリビュートに依存する SRTP と正常にネゴシエートするには、暗号パラメータが必要です。ネットワーク全体の暗号パラメータの整合性を確保するため、SRTP は SIPS スキーマ (sips:example.com) を使用します。Cisco IOS 音声ゲートウェイ、または Cisco Unified Border Element が、TLS 暗号化を使用し、TLS サポートを提供できないエンドポイントに invite を送信するように設定されている場合、そのエンドポイントは INVITE メッセージを拒否します。このような場合、ゲートウェイまたは Cisco UBE を、RTP のみのコールにフォールバックさせるか、コールを拒否するように設定できます。

SRTP に対する SIP サポート機能には次のセキュリティ上の利点があります。

- RTP パケットの機密保持：未承認のエントリによるパケット ペイロードの読み取りを防止し、承認済みのエントリからは秘密暗号キーを入力せずにパケット ペイロードを読み取れるようにします。
- RTP パケットのメッセージ認証：偽造、変更、または置換に対するパケットの整合性を保護します。
- リプレイ保護：DoS 攻撃からセッションアドレスを保護します。

表 1 に、TLS と SRTP が設定されている場合に生じる 4 つの組み合わせに応じた SIP INVITE メッセージのセキュリティ レベルの説明を示します。

表 1 TLS と SRTP の組み合わせ

TLS	SRTP	説明
オン	オン	シグナリングおよびメディアがセキュリティ保護される。
オフ	オン	シグナリングがセキュリティ保護される： <ul style="list-style-type: none"> <li>• <b>srtp fallback</b> コマンドを使用すると、ゲートウェイは RTP のみの SDP を送信します。</li> <li>• <b>srtp fallback</b> コマンドを設定しない場合、コールは失敗し、ゲートウェイは INVITE メッセージを送信しません。</li> </ul> (注) Cisco IOS リリース 12.4(20)T 以降 (および Cisco IOS リリース 12.4(22)T 以降の Cisco UBE) <b>srtp fallback</b> コマンドが設定されていない場合も SRTP のみを使用して (SIPS は使用せずに) 確立されたコールは成功します。

表 1 TLS と SRTP の組み合わせ (続き)

TLS	SRTP	説明
オン	オフ	RTP のみのコール
オフ	オフ	シグナリングおよびメディアはセキュリティ保護されない。

## 暗号パラメータ

RFC 3711 では、アトリビュート `a=crypto` を含む SRTP 暗号パラメータが定義されています (表 2 を参照してください)。これらのパラメータの一部は宣言型であり、宣言者の送信方向にしか適用されませんが、他のパラメータはネゴシエート可能であり、送受信の両方向に適用されます。

次に、暗号アトリビュート構文を示します。

```
a=crypto:<tag> <crypto-suite> <key-params> [<session-params>]
```

表 2 に、暗号アトリビュート構文の概要を示します。

表 2 暗号アトリビュート構文

アトリビュート	任意	説明
tag	なし	tag アトリビュートは、提供された複数の暗号アトリビュートのうち、返答で選択されたものを判別する特定の暗号アトリビュート ID で使用される一意の 10 進数です。
crypto-suite	なし	crypto-suite アトリビュートは、暗号化アルゴリズムおよび認証アルゴリズムを判別します。Cisco IOS 音声ゲートウェイおよび Cisco UBE は、デフォルトスイートである AES_CM_128_HMAC_SHA1_32 (128 ビット キー、および 32 ビット タグを持つ HMAC-SHA1 メッセージ認証を備えた AES-CM 暗号化) をサポートしています。
key-params	なし	"inline:" <key salt> [" " lifetime] [" " MKI ":" length] key salt は、Base64 符号化接続済みマスター キーおよびソルトです。
session-params	あり	session-params は、指定された転送に固有で、オプションのアトリビュートです。ゲートウェイは発信する INVITE メッセージ内に session-params を生成せず、SDP ライブラリはこの構文を解析しません。

## SDP ネゴシエーション

SRTP をサポートしないエンドポイント間のコールを成功させるには、`srtp` コマンドを設定して、SRTP に対する SIP サポートをイネーブルにできますが、一方または両方のエンドポイントで SRTP がサポートされていない場合は、RTP メカニズムへのフォールバックをイネーブルにすることもできます。SRTP がサポートされていない場合に、Cisco IOS 音声ゲートウェイまたは Cisco Unified Border Element を RTP にフォールバックするよう設定するには、`srtp fallback` コマンドをグローバルに、または個々のダイヤルピアで設定します。

`srtp` コマンドがイネーブルの場合、INVITE メッセージ内のオファー SDP が保持できる RTP/SAVP (RTP/セキュア AVP) 転送タイプの m 行は 1 行のみです。コールされたエンドポイントが SRTP をサポートしていない場合、コールは 4xx エラーにより失敗します。ただし、`srtp fallback` コマンドを設定すると、ゲートウェイはコールを失敗させるだけでなく、RTP のみのオファーを含む別の INVITE メッセージを生成します。



(注) Cisco IOS リリース 12.4(20)T 以降 (および Cisco IOS リリース 12.4(22)T 以降の Cisco UBE) **srtp fallback** コマンドが設定されていない場合も SRTP のみを使用して (SIPS は使用せずに) 確立されたコールは成功します。

ゲートウェイまたは Cisco Unified Border Element がコールされたエンドポイントの場合は、 $m$  行の値に SRTP のみ、RTP のみ、または SRTP と RTP の両方を持つオファーを受け入れます。2 行の  $m$  行 (SRTP と RTP) があるコールでは、設定がインバウンドダイヤルピアの設定とグローバルコンフィギュレーションのどちらかによって、ネゴシエーションが異なります。一方の  $m$  行のみがネゴシエートし、他方の  $m$  行のポート番号は 0 に設定されます。

表 3 に、ネゴシエーションの間のゲートウェイ動作の概要を示します。

表 3 ネゴシエーションの間のゲートウェイ動作

ダイヤルピアでの設定	SRTP で受信された INVITE メッセージ	SRTP と RTP で受信された INVITE メッセージ	RTP で受信された INVITE メッセージ
SRTP のみ	SRTP コール	SRTP コール、RTP の $m$ 行のポート番号が 0 に設定されます。	488 (未許可メディア)
フォールバックできる SRTP	SRTP コール	SRTP コール、RTP の $m$ 行のポート番号が 0 に設定されます。	RTP コール、SRTP の $m$ 行のポート番号が 0 に設定されます。
SRTP なし	488 (未許可メディア)	RTP コール、SRTP の $m$ 行のポート番号が 0 に設定されます。	RTP コール

次に、RTP/SAVP メディア転送タイプの暗号アトリビュートを使用し、2 行の  $m$  行を持つオファー SDP の例を示します。

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 7826 3751 IN IP4 172.18.193.98
s=SIP Call
c=IN IP4 172.18.193.98
t=0 0
m=audio 1789 RTP/AVP 0
a=rtpmap:0 PCMU/8000
m=audio 51372 RTP/SAVP 0
a=rtpmap:0 PCMU/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_32
inline:d0RmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHAwJSoj|2^20|1:32
```

次に、SRTP がサポートされている、対応する返答 SDP の例を示します。

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 7826 3751 IN IP4 172.18.193.98
s=SIP Call
c=IN IP4 172.18.193.98
t=0 0
m=audio 0 RTP/AVP 0
a=rtpmap:0 PCMU/8000
m=audio 49170 RTP/SAVP 0
a=crypto:1 AES_CM_128_HMAC_SHA1_32
inline:NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj|2^20|1:32
```

## 呼制御とシグナリング

SIP は、SRTP ライブラリを使用して暗号キーを受信します。コールに SRTP を設定し、暗号コンテキストがサポートされている場合、SDP は暗号パラメータを提供します。暗号パラメータが正常にネゴシエートされると、パケットの暗号化と復号化を行う DSP にパラメータがダウンロードされます。送信者は AES アルゴリズムを使用してペイロードを暗号化し、RTP パケットにカプセル化される認証タグを作成します。受信者は、認証タグを検証してペイロードを復号化します。

## SRTP のデフォルト設定および推奨設定

表 4 に SRTP のデフォルト設定および推奨設定を示します。

表 4 SRTP のデフォルト設定および推奨設定

パラメータ	デフォルト	推奨値
キー派生率	0	0 : キーの再生成をサポート
マスター キーの長さ	128 ビット	128 ビット
マスター ソルト キーの長さ	112 ビット	112 ビット
MKI インジケータ	0	0
MKI の長さ	0	0
PRF	AES_CM	128
セッション認証キーの長さ	128	128
セッション暗号キーの長さ	128 ビット	128 ビット
セッション ソルト キーの長さ	112	112
SRTP 認証	HMAC-SHA1	HMAC-SHA1
SRTCP 認証	HMAC-SHA1	HMAC-SHA1
SRTP 暗号	AES_CM	AES_CM
SRTCP 暗号	AES_CM	NULL
SRTP HMAC タグの長さ	80	32 (音声) : サポート対象 80 (その他) : サポート対象外
SRTCP HMAC タグの長さ	80	80
SRTP パケットの最大ライフタイム	2 <sup>48</sup> パケット	2 <sup>48</sup> パケット
SRTCP パケットの最大ライフタイム	2 <sup>31</sup> パケット	2 <sup>31</sup> パケット
SRTP リプレイウィンドウ サイズ	64	64 : サポート対象外
SRTCP リプレイウィンドウ サイズ	64	64 : サポート対象外

Cisco IOS 音声ゲートウェイまたは Cisco UBE で SRTP セッションが確立される前に、次の暗号化情報が 2 つのエンドポイント間の SDP で交換されている必要があります。

- クリプトスイート : 暗号アルゴリズム {AES\_CM\_128\_HMAC\_SHA1\_32} およびサポートされるコーデックのリスト {g711, G729, G729a}。クリプトスイートは、複数存在する場合があります。Cisco IOS リリース 12.4(15)T がサポートするのは、1 つのクリプトスイートのみです。
- クリプトコンテキスト : 16 バイトのマスター キーおよび 14 バイトのメッセージ ソルト。

## マスター キーの生成

SRTP ライブラリは、ランダム マスター キーを生成する API である `srtp_generate_master_key` を提供します。暗号化と認証に使用する場合、キーの長さは 128 ビットです（マスター キーおよびセッション キー）。また、RFC 3711 では「ソルティング キー」（マスター ソルトおよびセッション ソルト）が紹介されており、セッション キーのキー派生において、マスター キーを使用することが強く推奨されています。ソルティング キー（ソルト）は、事前計算攻撃およびタイム メモリ トレードオフ攻撃に対する防衛策として使用されます。

マスター ソルト（別名  $n$  ビット SRTP キー）は、キー派生時のオフライン キー コリジョン攻撃を回避しますが、これを使用する場合はランダムに（ただし公開で）使用する必要があります。マスター ソルトはマスター キーを基に生成され、セッション キーのキー派生時に使用されます。次に、セッション ソルトが付加的なストリーム サイファへのさまざまな攻撃に対抗するための暗号化に使用されます。すべてのソルティング キー（マスター ソルトおよびセッション ソルト）は、112 ビットです。

## SRTP オファーと返答の交換

ゲートウェイを SRTP およびエンドツーエンド TLS 対応に（グローバルに、または個々のダイヤル ピアで）設定する場合、発信 INVITE メッセージの SDP 内には暗号パラメータが含まれます。

**srtp fallback** コマンドを使用して、コールされたエンドポイントが SRTP をサポートしていない場合（オファーは 4xx クラス エラー応答で拒否されます）、ゲートウェイまたは Cisco Unified Border Element は、新しい INVITE 要求で、RTP オファー SDP を送信します。**srtp fallback** コマンドを設定しない場合、コールは失敗します。



(注) Cisco IOS リリース 12.4(20)T 以降（および Cisco IOS リリース 12.4(22)T 以降の Cisco UBE）**srtp fallback** コマンドが設定されていない場合も SRTP のみを使用して（SIPS は使用せずに）確立されたコールは成功します。

ゲートウェイ、または Cisco Unified Border Element が SRTP オファーを受信すると、ネゴシエーションは、指定されている場合はインバウンドダイヤル ピアに基づき、指定されていない場合はグローバル コンフィギュレーションに基づきます。複数の暗号アトリビュートが提供された場合は、ゲートウェイにより (AES\_CM\_128\_HMAC\_SHA1\_32) をサポートする SRTP オファーが選択されます。暗号アトリビュートには次の内容が含まれます。

- オファー内の受け入れられた暗号アトリビュートからのタグおよび同じクリプトスイート。
- SRTP ライブラリ API を使用してゲートウェイにより生成された一意のキー。
- すべてのネゴシエーション済みのセッションパラメータ、およびその宣言型パラメータのセット（存在する場合）。

この暗号スイートが提供されたアトリビュートのリストに含まれていない場合、または有効なアトリビュートがない場合、SRTP ネゴシエーションは失敗します。INVITE メッセージに代替 RTP オファーが含まれている場合、ゲートウェイ（または Cisco UBE）はネゴシエーションを実行し、コールは（ノンセキュア）RTP モードにフォールバックします。代替オファーがなく SRTP ネゴシエーションが失敗した場合、INVITE メッセージは 488 エラー（許可されていないメディア）で拒否されます。

## キー再生成のルール

SRTP ストリームではキーの再生成は発生しません。REINVITE/UPDATE メッセージは、メディア関連の情報（コーデック、宛先アドレス、ポート番号）またはコール保留のような他の機能を更新するため、確立された SIP コール内で使用されます。キーはオファー SDP に新しい接続アドレスまたはポー

トが含まれている場合にのみ生成される必要があります。ソース接続アドレスおよびポートは変更されないため、ゲートウェイまたは Cisco UBE はキーは STRP セッション向けにキーが作成された後は、新しいマスター キーを生成しません。

## コール機能の相互作用

ここでは、SRTP に対する SIP サポートが設定されている場合のコール機能の相互作用について説明します。

### コール保留

ゲートウェイが、初期コール セットアップのセキュリティが確保された後に、初回のコール保留 REINVITE メッセージを受信すると、ゲートウェイは既存の SRTP ストリームをホールドにし、200 OK メッセージ内のその返答はオファー SDP に依存します。オファーに暗号アトリビュートが含まれている場合、ゲートウェイはこの返答内の暗号アトリビュートを含めて応答します。

### シグナリング フォーキング

プロキシは SRTP オファーを持つ INVITE メッセージをフォーキングすることができ、200 OK メッセージを受信されるまでの間、複数の SRTP がストリームする可能性があります。ゲートウェイは常に最後の返答を受け入れるため、ゲートウェイにより以前の SRTP ストリームは削除され、最新のエンドポイントに対する新しいストリームが作成されます。他のエンドポイントもゲートウェイにストリームする可能性があります。DSP は最後のストリームのクリプトスイートおよびキーを認識するため、これらのパケットの認証は失敗し、パケットはドロップされます。

### コール リダイレクション

ゲートウェイは、プロキシまたはリダイレクト サーバに送信された INVITE メッセージに対し、リダイレクトされたコンタクトアドレスのリストを持つ 3xx 応答が返された場合、コールをリダイレクトします。ゲートウェイは 3xx メッセージのコンタクト内のスキーマに基づいて、3xx 応答を処理します。メッセージが SIP でありコールにフォールバックできる SRTP を設定している場合、ゲートウェイは SRTP のみのリダイレクトされた INVITE メッセージをオファーします。SRTP のみに対応するように設定した場合は、オファーも SRTP のみになります。

スキーマが SIP で、コールをフォールバックできる RTP に対応するコールの設定に **srtp fallback** コマンドを使用する場合、INVITE メッセージには RTP オファーが含まれます。**srtp fallback** コマンドを設定しない場合、コールは失敗します。



(注) Cisco IOS リリース 12.4(20)T 以降 (および Cisco IOS リリース 12.4(22)T 以降の Cisco UBE) **srtp fallback** コマンドが設定されていない場合も SRTP のみを使用して (SIPS は使用せずに) 確立されたコールは成功します。

### コール転送

SRTP に対する SIP サポート機能は、アウトバウンドダイヤル ピアまたはグローバル コンフィギュレーションに基づくコール転送と相互作用します。コール転送の間、INVITE メッセージを送信して、転送ターゲットへの接続を確立します。ゲートウェイは、アウトバウンドダイヤル ピアまたはグローバル コンフィギュレーションに SRTP オファーが含まれている場合、INVITE メッセージに SRTP オファーを含めます。



## T.38 ファックス

T.38 転送のサポート対象は User Datagram Protocol (UDP; ユーザ データグラム プロトコル) です。T.38 call は、RTP または SRTP 音声コールとして開始されますが、この音声コールが T.38 ファックスモードに切り替わるとファックス コールはセキュリティ保護されなくなります。ファックスが音声に戻されると、コールは初期の音声ステートに戻ります。

## 会議コール

会議コールでは、いずれのインバウンド ダイアル ピアおよびメッセージ本文にも一致しない着信 INVITE メッセージは、コンテナ内のアプリケーションに送信されます。会議アプリケーションは、PROGRESS または CONNECT イベントを介して、必要なネゴシエーションと返答を行います。

# SRTP に対する SIP サポートの設定方法

ゲートウェイまたは Cisco Unified Border Element で SRTP に対する SIP サポートを設定する前に、グローバルに、または個々のダイアル ピアで SIPS を設定することを強く推奨します。ダイアル ピアでの設定はグローバル コンフィギュレーションよりも優先されます。

ここでは、次の設定について説明します。

- 「SIPS のグローバルな設定」(P.9) (任意)
- 「ダイアル ピアにおける SIPS の設定」(P.10) (任意)
- 「SRTP および SRTP フォールバックのグローバルな設定」(P.11) (必須)
- 「ダイアル ピアにおける SRTP および SRTP フォールバックの設定」(P.12) (任意)

## SIPS のグローバルな設定

Cisco IOS 音声ゲートウェイまたは Cisco Unified Border Element 上で、セキュリティ保護された SIP (SIPS) をグローバルに設定するには、次の手順を実行します。

### 手順の概要

1. `enable`
2. `configure terminal`
3. `voice service {pots | voatm | vofr | voip}`
4. `sip`
5. `url sips`
6. `exit`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例: Router> enable	特権 EXEC モードを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。
ステップ 2	<b>configure terminal</b>  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。
ステップ 3	<b>voice service {pots   voatm   vofr   voip}</b>  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。
ステップ 4	<b>sip</b>  例: Router(conf-voi-serv)# sip	SIP コンフィギュレーション モードを開始します。
ステップ 5	<b>url sips</b>  例: Router(conf-serv-sip)# url sips	音声ゲートウェイまたは Cisco UBE のすべてのダイヤルピアに対する VoIP コールの URL の生成を SIPS 形式で指定します。
ステップ 6	<b>exit</b>  例: Router(conf-serv-sip)# exit	現在のモードを終了します。

## ダイヤル ピアにおける SIPS の設定

個別のダイヤル ピアでセキュリティ保護された SIP (SIPS) 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. **dial-peer voice tag {pots | vofr | voip}**
4. **voice-class sip url sips**
5. **exit**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Router> enable	特権 EXEC モードを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。
ステップ 2	<b>configure terminal</b>  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。
ステップ 3	<b>dial-peer voice tag {pots   vofr   voip}</b>  例： Router(config)# dial-peer voice 111 voip	ダイヤル ピア音声コンフィギュレーション モードを開始します。
ステップ 4	<b>voice-class sip url sips</b>  例： Router(config-dial-peer)# voice-class sip url sips	個別のダイヤル ピアに対する VoIP コールの URL の設定を SIPS 形式で指定します。
ステップ 5	<b>exit</b>  例： Router(config-dial-peer)# exit	現在のモードを終了します。

## SRTP および SRTP フォールバックのグローバルな設定

Cisco IOS 音声ゲートウェイまたは Cisco Unified Border Element 上で、SRTP および SRTP フォールバック動作をグローバルに設定するには、次の動作を設定します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **voice service {pots | voatm | vofr | voip}**
4. **srtp**
5. **srtp fallback**
6. **exit**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Router> enable	特権 EXEC モードを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。
ステップ 2	<b>configure terminal</b>  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。
ステップ 3	<b>voice service {pots   voatm   vofr   voip}</b>  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。
ステップ 4	<b>srtp</b>  例： Router(conf-voi-serv)# srtp	Secure RTP コールを設定します。
ステップ 5	<b>srtp fallback</b>  例： Router(conf-voi-serv)# srtp fallback	Secure RTP コールがエンドポイントでサポートされていないために失敗した場合は、RTP にフォールバックします。
ステップ 6	<b>exit</b>  例： Router(conf-voi-serv)# exit	現在のモードを終了します。

## ダイヤル ピアにおける SRTP および SRTP フォールバックの設定

グローバルな SRTP 設定よりも優先される、個別のダイヤル ピアでの SRTP および SRTP フォールバック動作の設定を実行するには、次の動作を実行します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag {pots | vofr | voip}**
4. **srtp**
5. **srtp fallback**
6. **exit**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Router> enable	特権 EXEC モードを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。
ステップ 2	<b>configure terminal</b>  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。
ステップ 3	<b>dial-peer voice tag {pots   vofr   voip}</b>  例： Router(config)# dial-peer voice 111 voip	ダイヤル ピア音声コンフィギュレーション モードを開始します。
ステップ 4	<b>srtsp</b>  例： Router(config-dial-peer)# srtsp	Secure RTP コールを設定します。
ステップ 5	<b>srtsp fallback</b>  例： Router(config-dial-peer)# srtsp fallback	Secure RTP コールがエンドポイントでサポートされていないために失敗した場合は、RTP にフォールバックします。
ステップ 6	<b>exit</b>  例： Router(config-dial-peer)# exit	現在のモードを終了します。

## SRTP に対する SIP サポート設定の設定例

次に、Cisco IOS 音声ゲートウェイまたは Cisco Unified Border Element でグローバルに SIPS を設定する例を示します。

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# url sips
Router(conf-serv-sip)# exit
```

次に、ダイヤル ピア 111 で SIPS を設定する例を示します。

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# dial-peer voice 111 voip
Router(config-dial-peer)# voice-class sip url sips
Router(config-dial-peer)# exit
```

次に、RTP へのフォールバック機能を備えた SRTP を、Cisco IOS 音声ゲートウェイ、または Cisco Unified Border Element でグローバルに設定する例を示します。

```
Router> enable
```

```

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# voice service voip
Router(conf-voi-serv)# srtp
Router(conf-voi-serv)# srtp fallback
Router(conf-voi-serv)# exit

```

次に、RTP へのフォールバック機能を備えた SRTP をダイヤル ピア 111 で設定する例を示します。

```

Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# dial-peer voice 111 voip
Router(config-dial-peer)# srtp
Router(config-dial-peer)# srtp fallback
Router(config-dial-peer)# exit

```

## その他の参考資料

次の項では、SRTP に対する SIP サポート機能の設定に関連する参考資料を示します。

## 関連資料

関連項目	参照先
Cisco IOS ダイヤル ピアの概要	『 <a href="#">Dial Peer Overview</a> 』
Cisco IOS ダイヤル テクノロジー コマンド情報	『 <a href="#">Cisco IOS Dial Technologies Command Reference</a> 』
Cisco IOS SIP の機能 (リリース順リスト)	『 <a href="#">SIP Features Roadmap</a> 』
Cisco IOS SIP の概要と関連資料	『 <a href="#">Overview of SIP</a> 』
Cisco IOS ソフトウェアのコンフィギュレーション ガイド	<ul style="list-style-type: none"> <li>『<a href="#">Cisco IOS Dial Technologies Configuration Guide</a>』</li> <li>『<a href="#">Cisco IOS SIP Configuration Guide</a>』</li> </ul> <p>(注) 使用している Cisco IOS ソフトウェア リリースのコンフィギュレーション ガイドを検索するには、<a href="#">製品サポート</a> ページの <b>Cisco IOS および NX-OS ソフトウェア</b> カテゴリを選択し、リリースに基づいて目的のページにアクセスします (<a href="http://www.cisco.com/web/psa/products/index.html">http://www.cisco.com/web/psa/products/index.html</a>)。</p>
Cisco IOS 音声コマンド情報	『 <a href="#">Cisco IOS Voice Command Reference</a> 』
Cisco IOS 音声設定情報	<a href="#">Cisco IOS Voice Configuration Library</a>
Cisco Unified Border Element の構成情報	『 <a href="#">Cisco Unified Border Element Configuration Guide</a> 』
Cisco Unified CME のコマンド情報	『 <a href="#">Cisco Unified Communications Manager Express Command Reference</a> 』
Cisco Unified CME の構成情報	<a href="#">Cisco Unified CME Support Documentation Home Page</a>

## RFC

RFC	
draft-ietf-mmusic-sdescriptions-08.txt	『 <a href="#">Session Description Protocol Security Descriptions for Media Streams</a> 』

RFC	
RFC 3263	「 <i>Session Initiation Protocol (SIP): Locating SIP Servers</i> 」
RFC 3711	「 <i>The Secure Real-time Transport Protocol (SRTP)</i> 」

## MIB

MIB	MIB リンク
なし	<p>選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## シスコのテクニカル サポート

説明	リンク
<p>Cisco Support Web サイトには、資料やツールなど幅広いオンライン リソースが用意されており、シスコの製品およびテクノロジーに関するトラブルシューティングや技術的な問題の解決などに役立てることができます。</p> <p>以下を含むさまざまな作業にこの Web サイトが役立ちます。</p> <ul style="list-style-type: none"> <li>• テクニカル サポートを受ける</li> <li>• ソフトウェアをダウンロードする</li> <li>• セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける</li> <li>• ツールおよびリソースへアクセスする</li> <li>• Product Alert の受信登録</li> <li>• Field Notice の受信登録</li> <li>• Bug Toolkit を使用した既知の問題の検索</li> <li>• Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する</li> <li>• トレーニング リソースへアクセスする</li> <li>• TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する</li> </ul> <p>Japan テクニカル サポート Web サイトでは、Technical Support Web サイト (<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>) の、利用頻度の高いドキュメントを日本語で提供しています。Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。</p> <p><a href="http://www.cisco.com/jp/go/tac">http://www.cisco.com/jp/go/tac</a></p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## SRTP に対する SIP サポート設定に関する機能情報

表 5 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。Cisco IOS リリース 12.2(1)、Cisco IOS リリース 12.2(1)、12.0(3)S、またはこの表に掲載されているリリース以降で変更または導入された機能のみを示します。

ここに掲載されていない機能に関する情報については、『[Cisco IOS SIP Features Roadmap](http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-roadmap.html)』([http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip\\_cg-roadmap.html](http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-roadmap.html)) を参照してください。

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。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator により、どの Cisco IOS および Catalyst OS ソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスしてください。Cisco.com のアカウントは必要ありません。



(注) 表 5 には、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 Cisco IOS ソフトウェア リリースでもサポートされます。

表 5 SRTP に対する SIP サポート設定に関する機能情報

機能名	リリース	機能情報
SRTP に対する SIP サポート	12.4(15)T	この機能により、フックフラッシュ (HF) Cisco 音声ゲートウェイ上で、FXS 電話を使用するコール保留、コールウェイティング、およびコール会議 (3WC) などの付加的なサービス機能に対する SIP サポートが導入されます。 次のコマンドが導入または変更されました。 <b>srtp、srtp fallback</b>
ノンセキュア RTP への SIP SRTP フォールバック	12.4(15)XY 12.4(20)T	この機能により、Cisco IOS 音声ゲートウェイにおける、既存の SRTP の RTP へのフォールバックを拡張し、遅延したオファーをサポートしたり、SRTP over SIP のサポートを追加したりすることができます。 次のコマンドが導入または変更されました。 <b>srtp negotiate、voice-class sip srtp negotiate</b>
SIP および H323 向け Secure RTP コールのインターワーキング	12.4(20)T	この機能により、Secure RTP (SRTP) コールを H323 から SIP および SIP から SIP に接続できるオプションが提供されます。また、この機能は SRTP のフォールバック サポートを Cisco IOS 音声ゲートウェイから Cisco Unified Border Element に拡張します。 この機能では、新しいコマンド、または変更されたコマンドは使用していません。



表 5 SRTP に対する SIP サポート設定に関する機能情報 (続き)

機能名	リリース	機能情報
Cisco Unified Border Elements 向けノンセキュア RTP への SIP SRTP フォールバック	12.4(22)T	<p>この機能により、SRTP から、遅延したオファーを含む RTP へのフォールバック、および Cisco Unified Border Element への SIP 上における SRTP の両方のサポートが追加されます。</p> <p>この機能では、新しいコマンド、または変更されたコマンドは使用していません。</p>
SRTP-RTP インターネットワーキングの Cisco Unified Border Element サポート	12.4(22)YB	<p>この機能により、Cisco Unified Border Element の一方の IP 区間上の SRTP から、他方の IP 区間上の RTP へのインターネットワーキングをサポートする機能が提供されます。</p> <p>コマンド <b>tls</b> が導入または変更されました。</p>

## 用語集

**AVP** : Audio/Video Profile (オーディオ/ビデオ プロファイル)。

**CAC** : Call Admission Control (コール アドミッション制御)。

**CME** : Communications Manager Express。

**CVP** : Customer Voice Portal。

**GW** : ゲートウェイ。

**ISDN** : Integrated Services Digital Network (サービス総合デジタル ネットワーク)。

**MIME** : Multipurpose Internet Mail Extensions。

**m line** : メディア ストリームに関する情報を制限する行。SDP セッションのメディア レベル セクションが、この行で開始および終了される。

**MOH** : Music On Hold (保留音)。

**OGW** : 発信側ゲートウェイ (入力ゲートウェイ)。

**PBX** : Private Branch Exchange (構内交換機)。

**PINX** : Private Integrated Services Network Exchange。

**PISN** : Private Integrated Services Network。

**QoS** : Quality Of Service (サービス品質)。

**QSIG** : Q シグナリング プロトコル。

**RSVP** : Resource Reservation Protocol (リソース予約プロトコル)。

**RTP** : Real-time Transport Protocol (リアルタイム トランスポート プロトコル)。

**SDP** : Session Description Protocol (セッション記述プロトコル)。

**SIP** : Session Initiation Protocol (セッション開始プロトコル)。

**SRTP** : Secure Real-time Transport Protocol。

**TDM** : Time-Division Multiplexing (時分割多重)。

**TGW** : 終端ゲートウェイ (出力ゲートウェイ)。

**UA** : User Agent (ユーザ エージェント)。

**UDP** : User Datagram Protocol (ユーザ データグラム プロトコル)。

**URI** : Uniform Resource Identifier (ユニフォーム リソース識別子)。

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

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

© 2007–2009 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2007–2010, シスコシステムズ合同会社.  
All rights reserved.

