Cisco SRST での SIP/TLS/TCP セキュア コール シグナリングと SRTP メディア暗号化の設定

Configuring SIP/TLS/TCP Secure Call Signaling and SRTP Media Encryption with Cisco SRST

OL-20685-01-J

【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。米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

この機能を使用すると、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かつ暗号化された接続を確立できます。

機能に関する情報

使用しているソフトウェア リリースで、このモジュールに記載されたすべての機能がサポートされないことがあります。機能の最新情報と問題点については、プラットフォームとソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載された機能と、各機能がサポートされたリリースのリストについては、「Cisco SRST での SIP/TLS/TCP セキュア コール シグナリングと SRTP メディア暗号化に関する機能情報」（P.11）を参照してください。

Cisco Feature Navigator を使用して、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 イメージのサポートに関する情報を入手します。Cisco Feature Navigator にアクセスするには、http://www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

内容

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

Cisco SRST での SIP/TLS/TCP セキュア コール シグナリングと SRTP メディア暗号化の設定に関する情報

Cisco IP Phone ファームウェア アップデート 8.5(3) および Cisco IOS リリース 15.0(1)XA 以降、Cisco SRST は SIP/UDP 接続と SIP/TLS/TCP 接続をサポートするようになりました。また、Cisco SRST は、IP 電話機のセキュリティ設定に基づいて RTP および SRTP メディア接続をサポートするようになりました。

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。

- 基本的なコーリング
- 保留 / 復帰
- 会議
- 転送
- ブラインド転送
- 自動転送

Cisco SRST の SIP-to-Other は、基本的なコーリングだけをサポートします（ただし、他の機能が動作することがあります）。

セキュアなコール シグナリングの設定方法

この項には次のタスクが含まれます。

Cisco Unified Communications Manager の設定

Cisco Unified Communications Manager では、セキュアなエンドポイントとセキュアでないエンドポイントがそれぞれ別の SRST 参照設定とデバイス プールを持つ必要があります。

Cisco Unified Communications Manager Administration で [System] > [SRST] と選択し、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、[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、[Is SRST Secure?] をオンにするかどうかは Skinny Call Control Protocol（SCCP）の設定に応じて異なります。SIP ポートは 5060（デフォルト値）である必要があります。

[Device] > [Phone] と選択して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。

SRTP の設定

この項では、Cisco SRST で SRTP を設定する方法について説明します。

手順の要約

1. **enable**
2. **configure terminal**
3. **service voip**
4. **srtp fallback**
5. **allow-connections sip to h323**
6. **allow-connections sip to sip**

詳細な手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 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。
ステップ 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。
ステップ 4	**srtp fallback** **例：** `Router(config-voi-serv)# srtp fallback`	SRTP を使用してセキュアなコールとコール フォールバックを有効にするよう指定します。
ステップ 5	**allow-connections sip to h323** **例：** `Router(config-voi-serv)# allow-connections sip to h323`	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。
ステップ 6	**allow-connections sip to sip** **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。

セキュアなモードの設定

この項では、Cisco SRST でセキュリティなモードを設定する方法について説明します。

手順の要約

1. **sip**
2. **url sip | sips**
3. **srtp negotiate cisco**
4. **exit**
5. **exit**

詳細な手順

	コマンドまたはアクション	目的
ステップ 1	**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。
ステップ 2	**url sip | sips** **例：** `Router(conf-serv-sip)# url sips`	セキュアな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。
ステップ 3	**srtp negotiate cisco** **例：** `Router(conf-serv-sip)# srtp negotiate cisco`	SRTP オファーの応答時に 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。
ステップ 4	**exit** **例：** `Router(conf-serv-sip)# exit`	音声サービス コンフィギュレーション モードに戻ります。
ステップ 5	**exit** **例：** `Router(conf-voi-serv)# exit`	グローバル コンフィギュレーション モードに戻ります。

TLS の設定

この項では、Cisco SRST で TLS を設定する方法について説明します。

手順の要約

1. **voice register global**
2. **security-policy secure**
3. **exit**

詳細な手順

	コマンドまたはアクション	目的
ステップ 1	**voice register global** **例：** `Router(config)# voice register global`	音声登録グローバル コンフィギュレーション モードを開始します。
ステップ 2	**security-policy secure** **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。
ステップ 3	**exit** **例：** `Router(config-register-global)# exit`	グローバル コンフィギュレーション モードに戻ります。

厳密な暗号化の設定

この項では、Cisco SRST で厳密な暗号化を設定する方法について説明します。

手順の要約

1. **sip-ua**
2. **registrar ipv4**:*destination-address* **expires** *seconds*
3. **xfer target dial-peer**
4. **crypto signaling default trustpoint** *string* [**strict-cipher**]
5. **end**

詳細な手順

	コマンドまたはアクション	目的
ステップ 1	**sip-ua** **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。
ステップ 2	**registrar ipv4:***destination-address* **expires** *seconds* **例：** `Router(config-sip-ua)# registrar ipv4:192.0.2.10 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。*destination-address* はプライマリ SIP レジストラ サーバの IP アドレスです。
ステップ 3	**xfer target dial-peer** **例：** `Router(config-sip-ua)# refer 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。
ステップ 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; 公開鍵インフラストラクチャ）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; 高度暗号化規格 128）Cipher-Block-Chaining（CBC）Secure Hash Algorithm（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。
ステップ 5	**end** **例：** `Router(config-sip-ua)# end`	現在の設定セッションを終了し、特権 EXEC モードに戻ります。

設定の検証

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、コンタクト 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       192.0.2.108    388           192.0.2.108
    TLS           00120014-4ae40064-f1a3e9fe-8d301072@192.0.2.1
                  40004
    3029993       192.0.2.103    382           192.0.2.103
    TCP           001bd433-1c840052-655cd596-4e992eed@192.0.2.1
```

```
                40011
3029982         192.0.2.106     406             192.0.2.106
UDP             001d452c-dbba0056-0481d321-1f3f848d@192.0.2.1
                40001
3029983         192.0.2.106     406             192.0.2.106
UDP             001d452c-dbba0057-1c69b699-d8dc6625@192.0.2.1
                40003
3029992         192.0.2.107     414             192.0.2.107
TLS             001e7a25-50c9002c-48ef7663-50c71794@192.0.2.1
                40005
```

特権 EXEC モードで **show voice register global** コマンドを使用すると、SIP 電話機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=7.1]
    ========================
    Version 7.1
    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
    System message is Welcome to ALOA Secure Fallback
    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#
```

追加の参照資料

次の項では、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	ドキュメント タイトル
Cisco Unified SRST の設定	• *Cisco Unified SIP SRST System Administrator Guide* • *Cisco Unified SRST System Administrator Guide* • *Cisco Unified SRST and SIP SRST Command Reference*
Cisco IOS 音声設定	• *Cisco IOS Voice Configuration Library* • *Cisco IOS Voice Command Reference*

標準

標準	タイトル
この機能では新しい標準や変更された標準はサポートされず、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB リンク
この機能では新しい MIB や変更された MIB はサポートされず、既存の MIB のサポートは変更されていません。	選択され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 を見つけてダウンロードするには、次の URL に存在する Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能では新しい RFC や変更された RFC はサポートされず、既存の RFC のサポートは変更されていません。	—

シスコのテクニカル サポート

説明	リンク
シスコ サポート Web サイトは、シスコの製品およびテクノロジーで発生した技術的な問題をトラブルシューティングおよび解決するためのドキュメンテーションとツールを含む広範なオンライン リソースを提供します。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 テクニカル サポートを受ける ソフトウェアをダウンロードする セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ツールおよびリソースへアクセスする Product Alert の受信登録 Field Notice の受信登録 Bug Toolkit を使用した既知の問題の検索 Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する トレーニング リソースへアクセスする TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する Japan テクニカル サポート Web サイトでは、Technical Support Web サイト（ http://www.cisco.com/techsupport ）の、利用頻度の高いドキュメントを日本語で提供しています。Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。 http://www.cisco.com/jp/go/tac	http://www.cisco.com/techsupport

コマンド リファレンス

次のコマンドは、このモジュールに記載された機能で導入または変更されました。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、Command Lookup Tool（http://tools.cisco.com/Support/CLILookup）を使用するか、または『*Cisco IOS Master Command List, All Releases*』（http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html）を参照してください。

- **crypto signaling**
- **security-policy**
- **show sip ua status**

- **show voice register global**
- **srtp negotiate**
- **xfer target dial-peer**

Cisco SRST での SIP/TLS/TCP セキュア コール シグナリングと SRTP メディア暗号化に関する機能情報

表 1 は、この機能のリリース履歴を示しています。

使用している Cisco IOS ソフトウェア リリースですべてのコマンドを利用できるわけではありません。特定のコマンドのリリース情報については、コマンド リファレンス ドキュメンテーションを参照してください。

Cisco Feature Navigator を使用して、プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手してください。Cisco Feature Navigator を使用すると、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 Cisco IOS と Catalyst OS ソフトウェア イメージを調べることができます。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 1 は、特定の Cisco IOS ソフトウェア リリース トレインの特定の機能がサポートされた Cisco IOS だけを示しています。特に記述がない限り、Cisco IOS ソフトウェア リリース トレインの後続リリースでも、該当する機能がサポートされます。

表 1　Cisco SRST での SIP/TLS/TCP セキュア コール シグナリングと SRTP メディア暗号化に関する機能情報

機能名	リリース	機能情報
Cisco SRST での SIP/TLS/TCP セキュア コール シグナリングと SRTP メディア暗号化の設定に関する情報	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。導入または変更されたコマンド：**crypto signaling**, **security-policy, show sip ua status, show voice register global, srtp negotiate, xfer target dial-peer**

用語集

RTP：Real-Time Transport Protocol。IP パケットスイッチド ネットワークにリアルタイム データを配信します。

SCCP：Skinny Call Control Protocol。特定のクライアントと Cisco Unified Communications Manager 間の通信プロトコルです。

SIP：Session Initiation Protocol。音声コールなどのマルチメディア サービスを設定、保守、および終了するためのインターネット プロトコルです。

SRST：Survivable Remote Site Telephony。Cisco Unified Communications Manager に、ローカル ネットワーク上のシスコ 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。

SRTP：Secure Real-time Transport Protocol。RTP に対して暗号化とメッセージ認証を提供します。

TCP：Transmission Control Protocol。インターネット プロトコルの TCP/IP スイートの一部であるトランスポート レイヤ プロトコルです。

TLS：Transport Layer Security。公開鍵暗号化を使用するセキュリティ プロトコルです。

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や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。

© 2009 Cisco Systems, Inc.
All rights reserved.

Copyright © 2009–2010, シスコシステムズ合同会社 .
All rights reserved.