



Survivable Remote Site Telephony (SRST) リファレンスのセキュリティ 設定

この章は、次の内容で構成されています。

- [SRST のセキュリティの概要 \(P.12-2\)](#)
- [SRST のセキュリティ設定用チェックリスト \(P.12-3\)](#)
- [SRST リファレンスのセキュリティ設定 \(P.12-4\)](#)
- [SRST リファレンスのセキュリティの設定内容 \(P.12-6\)](#)
- [セキュア SRST リファレンスのトラブルシューティング \(P.12-7\)](#)
- [その他の情報 \(P.12-7\)](#)

SRST のセキュリティの概要

SRST 対応ゲートウェイは、Cisco CallManager がコールを完了できない場合に、制限付きのコール処理タスクを提供します。保護された SRST 対応ゲートウェイには、自己署名証明書が含まれています。Cisco CallManager Administration で SRST 設定作業を実行した後、Cisco CallManager は TLS 接続を使用して SRST 対応ゲートウェイで Certificate Provider サービスを認証します。

次に、Cisco CallManager は SRST 対応ゲートウェイから証明書を取得して、その証明書を Cisco CallManager データベースに追加します。

Cisco CallManager Administration で従属デバイスをリセットすると、TFTP サーバは SRST 対応ゲートウェイの証明書を電話機の cnf.xml ファイルに追加してファイルを電話機に送信します。これで、保護された電話機は TLS 接続を使用して SRST 対応ゲートウェイと対話します。



ヒント

電話機設定ファイルには、単一の発行者からの証明書だけが含まれます。そのため、HSRP はサポートされません。

次の基準が満たされることを確認します。この基準を満たすと、保護された電話機と SRST 対応ゲートウェイとの間で TLS ハンドシェイクが行われます。

- SRST リファレンスに自己署名証明書が含まれている。
- Cisco CTL クライアントを介してクラスタをセキュア モードに設定した。
- 電話機に認証または暗号化を設定した。
- Cisco CallManager Administration で SRST リファレンスを設定した。
- SRST の設定後に、SRST 対応ゲートウェイおよび従属する電話機をリセットした。

クラスタセキュリティモードがノンセキュアになっている場合は、Cisco CallManager Administration でデバイスセキュリティモードが認証済みまたは暗号化済みと示されていても、電話機の設定ファイルのデバイスセキュリティモードはノンセキュアのままです。このような場合、電話機は、クラスタ内で SRST 対応ゲートウェイおよび Cisco CallManager サーバとのノンセキュア接続を試行します。

クラスタセキュリティモードがノンセキュアになっている場合は、デバイスセキュリティモードや IS SRST Secure? チェックボックスなど、Cisco CallManager Administration 内のセキュリティ関連の設定が無視されます。Cisco CallManager Administration 内の設定は削除されませんが、セキュリティは提供されません。

電話機が SRST 対応ゲートウェイへのセキュア接続を試行するのは、クラスタセキュリティモードが Secure Mode で、電話機設定ファイル内のデバイスセキュリティモードが認証済みまたは暗号化済みを設定されており、SRST Configuration ウィンドウで Is SRST Secure? チェックボックスがオンになっている、電話機の設定ファイル内に有効な SRST 証明書が存在する場合だけです。



ヒント

前のリリースの Cisco CallManager でセキュア SRST リファレンスを設定した場合は、Cisco CallManager のアップグレード時にその設定が自動的に移行されます。



(注) 暗号化済みまたは認証済みモードの電話機が SRST にフェールオーバーし、SRST での接続中に Cisco CallManager クラスタがセキュア モードからノンセキュア モードに切り替わった場合、これらの電話機は自動的に Cisco CallManager にフォールバックされません。管理者が SRST ルータの電源を切り、強制的にこれらの電話機を Cisco CallManager に再登録する必要があります。電話機が Cisco CallManager にフォールバックした後、管理者は SRST の電源を投入でき、フェールオーバーおよびフォールバックが再び自動になります。

SRST のセキュリティ設定用チェックリスト

表 12-1 を使用して、SRST のセキュリティ設定手順を進めます。

表 12-1 SRST のセキュリティ設定用チェックリスト

設定手順	関連手順および関連項目
ステップ 1 SRST 対応ゲートウェイに必要なすべての作業を実行したことを確認します。すべてを実行すると、デバイスが Cisco CallManager およびセキュリティをサポートします。	このバージョンの Cisco CallManager をサポートする『Cisco IOS SRST Version 3.3 System Administrator Guide』。これは、次の URL で入手できます。 http://www.cisco.com/univercd/cc/td/doc/product/voice/srst/srst33/srst33ad/index.htm
ステップ 2 Cisco CTL クライアントのインストールおよび設定に必要なすべての作業を実行したことを確認します。	Cisco CTL クライアントの設定 (P.3-1)
ステップ 3 電話機に証明書が存在することを確認します。	使用中の電話機モデルの Cisco IP Phone マニュアルを参照してください。
ステップ 4 電話機に認証または暗号化を設定したことを確認します。	SCCP または SIP 電話機セキュリティ プロファイルの適用 (P.5-9)
ステップ 5 Cisco CallManager Administration で SRST リファレンスにセキュリティを設定します。これには、Device Pool Configuration ウィンドウで SRST リファレンスを有効にする作業も含まれます。	SRST リファレンスのセキュリティ設定 (P.12-4)
ステップ 6 SRST 対応ゲートウェイと電話機をリセットします。	SRST リファレンスのセキュリティ設定 (P.12-4)

SRST リファレンスのセキュリティ設定

Cisco CallManager Administration で SRST リファレンスを追加、更新、または削除する前に、次の点を考慮してください。

- 保護された SRST リファレンスの追加：初めて SRST リファレンスにセキュリティを設定する場合、表 12-2 で説明するすべての項目を設定する必要があります。
- 保護された SRST リファレンスの更新：Cisco CallManager Administration で SRST の更新を実行しても、SRST 対応ゲートウェイの証明書は自動的に更新されません。証明書を更新するには、Update Certificate ボタンをクリックする必要があります。クリックすると証明書の内容が表示され、証明書を受け入れるか拒否する必要があります。証明書を受け入れると、Cisco CallManager はクラスタ内の各サーバで、信頼できるフォルダにある SRST 対応ゲートウェイの証明書を置き換えます。
- 保護された SRST リファレンスの削除：保護された SRST リファレンスを削除すると、Cisco CallManager データベースおよび電話機の cnf.xml ファイルから SRST 対応ゲートウェイの証明書が削除されます。

SRST リファレンスを削除する方法については、『Cisco CallManager アドミニストレーションガイド』を参照してください。

SRST リファレンスのセキュリティを設定するには、次の手順を実行します。

手順

ステップ 1 Cisco CallManager Administration で **System > SRST** の順に選択します。

ステップ 2 次の作業のどちらかを実行します。

- 新しい SRST リファレンスを追加するには、**Add New** ボタンをクリックし、**ステップ 3** に進みます。
- 既存の SRST リファレンスをコピーするには、『Cisco CallManager アドミニストレーションガイド』の説明に従って適切な SRST リファレンスを見つけ、コピーするリファレンスの横に表示されている **Copy** ボタンをクリックして、**ステップ 3** に進みます。
- 既存の SRST リファレンスを更新するには、『Cisco CallManager アドミニストレーションガイド』の説明に従って適切な SRST リファレンスを見つけ、**ステップ 3** に進みます。

ステップ 3 表 12-2 の説明に従い、セキュリティ関連の設定を入力します。

その他の SRST リファレンス設定内容の説明については、『Cisco CallManager アドミニストレーションガイド』を参照してください。

ステップ 4 Is SRST Secure? チェックボックスをオンにすると、Update Certificate ボタンをクリックして SRST 証明書をダウンロードする必要があるというメッセージがダイアログボックスに表示されます。**OK** をクリックします。

ステップ 5 **Save** をクリックします。

ステップ 6 データベース内の SRST 対応ゲートウェイの証明書を更新するには、**Update Certificate** ボタンをクリックします。



ヒント このボタンは、Is SRST Secure? チェックボックスをオンにして Save をクリックした後にだけ表示されます。

ステップ 7 証明書のフィンガープリントが表示されます。証明書を受け入れるには、**Save** をクリックします。

ステップ 8 **Close** をクリックします。

ステップ 9 SRST Reference Configuration ウィンドウで、**Reset** をクリックします。

追加の手順

Device Pool Configuration ウィンドウで SRST リファレンスが有効になったことを確認します。




追加情報

詳細については、[P.12-7](#) の「[関連項目](#)」を参照してください。

SRST リファレンスのセキュリティの設定内容

表 12-2 で、保護された SRST リファレンスに対して Cisco CallManager Administration で使用できる設定について説明します。

表 12-2 SRST リファレンスのセキュリティの設定内容

設定	説明
Is SRST Secure?	<p>SRST 対応ゲートウェイに、自己署名証明書が含まれることを確認した後、このチェックボックスをオンにします。</p> <p>SRST を設定してゲートウェイおよび従属する電話機をリセットすると、Cisco CTL Provider サービスは SRST 対応ゲートウェイで Certificate Provider サービスに認証を受けます。Cisco CTL クライアントは SRST 対応ゲートウェイから証明書を取得して、その証明書を Cisco CallManager データベースに格納します。</p> <p></p> <p>ヒント データベースおよび電話機から SRST 証明書を削除するには、このチェックボックスをオフにして Save をクリックし、従属する電話機をリセットします。</p>
SRST Certificate Provider Port	<p>このポートは、SRST 対応ゲートウェイ上で Certificate Provider サービスに対する要求を監視します。Cisco CallManager はこのポートを使用して SRST 対応ゲートウェイから証明書を取得します。Cisco SRST Certificate Provider のデフォルトポートは 2445 です。</p> <p>SRST 対応ゲートウェイ上でこのポートを設定した後、このフィールドにポート番号を入力します。</p> <p></p> <p>ヒント ポートが現在使用中の場合や、ファイアウォールを使用してファイアウォール内のポートを使用できない場合には、異なるポート番号の設定が必要になることもあります。</p>
Update Certificate	<p></p> <p>ヒント このボタンは、Is SRST Secure? チェックボックスをオンにして Save をクリックした後にだけ表示されます。</p> <p>このボタンをクリックすると、Cisco CTL クライアントは Cisco CallManager データベースに格納されている既存の SRST 対応ゲートウェイの証明書を置き換えます（証明書がデータベースに存在する場合）。従属する電話機をリセットした後、TFTP サーバは cnf.xml ファイルを（新しい SRST 対応ゲートウェイの証明書と共に）電話機に送信します。</p>

セキュア SRST リファレンスのトラブルシューティング

この項では、次のトピックについて取り上げます。

- [SRST リファレンスからのセキュリティの削除 \(P.12-7\)](#)
- [SRST リファレンスの設定時に表示されるセキュリティ メッセージ \(P.12-7\)](#)
- [SRST 証明書がゲートウェイから削除された場合のトラブルシューティング \(P.12-7\)](#)

SRST リファレンスからのセキュリティの削除

セキュリティの設定後に SRST リファレンスをノンセキュアにするには、Cisco CallManager Administration の SRST Configuration ウィンドウで、**Is the SRTS Secure?** チェックボックスをオフにします。ゲートウェイ上のクレデンシャル サービスを無効にする必要がある旨のメッセージが表示されます。

SRST リファレンスの設定時に表示されるセキュリティ メッセージ

Cisco CallManager Administration でセキュア SRST リファレンスを設定するときに、メッセージ「Port Numbers can only contain digits.」が表示される場合があります。

このメッセージは、SRST Certificate Provider Port を設定するときに、不正なポート番号を入力した場合に表示されます。ポート番号は、1024 ~ 49151 の範囲に存在する必要があります。

SRST 証明書がゲートウェイから削除された場合のトラブルシューティング

SRST 証明書が SRST 対応のゲートウェイから削除されている場合は、その SRST 証明書を Cisco CallManager データベースと IP Phone から削除する必要があります。

この作業を実行するには、SRST Configuration ウィンドウで、**Is the SRST Secure?** チェックボックスをオフにして **Update** をクリックし、**Reset Devices** をクリックします。

その他の情報

関連項目

- [SRST のセキュリティの概要 \(P.12-2\)](#)
- [SRST のセキュリティ設定用チェックリスト \(P.12-3\)](#)
- [SRST リファレンスのセキュリティ設定 \(P.12-4\)](#)
- [SRST リファレンスのセキュリティの設定内容 \(P.12-6\)](#)
- [セキュア SRST リファレンスのトラブルシューティング \(P.12-7\)](#)

シスコの関連マニュアル

- *Cisco IOS SRST Version 3.3 System Administrator Guide*
- *Cisco CallManager アドミニストレーションガイド*

