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

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、自己署名証明書または認証局が発行した証明書が含まれます。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 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　Cisco CallManager では、SRST 証明書に対して深度 1 のチェーニングだけをサポートします。つまり、電話機の設定ファイルには単一の発行者による証明書しか含まれません。この場合、システムは HSRP をサポートしません。

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、自己署名証明書または認証局が発行した証明書が含まれる。
- Cisco CTL クライアントを介してクラスタを混合モードに設定した。
- 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 Mixed 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に設定されており、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て、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。

関連項目

- SRST のセキュリティ設定用チェックリスト（P.7-4）
- SRST リファレンスのセキュリティ設定（P.7-5）
- SRST リファレンスのセキュリティ設定（P.7-7）
- トラブルシューティング（P.9-1）

SRST のセキュリティ設定用チェックリスト

表 7-1 を使用して、SRST のセキュリティ設定手順を進めます。

表 7-1　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 対応ゲートウェイで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。	• ローカルで有効な証明書が IP Phone 上に存在することの確認（P.9-42） • Manufacture-Installed Certificate（MIC）が IP Phone 内に存在することの確認（P.9-43）
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。	デバイス セキュリティ モードの設定（P.5-7）
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.7-5）
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.7-5）

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 7-2 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 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 SRST 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 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 証明書が削除されます。

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。

- 初めて SRST リファレンスを追加する。この作業を実行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。
- セキュリティを設定する SRST リファレンスを検索する。SRST リファレンスの検索については、『*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。既存の SRST リファレンスにセキュリティを設定して更新するには、表 7-2 を使用してください。

ステップ 3　SRST リファレンスを追加したか、更新したかに応じて、**Insert** または **Update** をクリックします。

ステップ 4　データベース内の SRST 証明書を更新するには、**Update SRST Certificate** ボタンをクリックします。

ヒント　このボタンは、既存の SRST リファレンスを更新する場合にだけ表示されます。

ステップ 5　**Reset Devices** をクリックします。

ステップ 6　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。

関連項目

- SRST のセキュリティの概要（P.7-2）
- SRST のセキュリティ設定用チェックリスト（P.7-4）
- SRST リファレンスのセキュリティ設定（P.7-7）
- トラブルシューティング（P.9-1）

SRST リファレンスのセキュリティ設定

表 7-2 を使用して、SRST リファレンスのセキュリティを設定します。

表 7-2　SRST リファレンスのセキュリティ設定

設定	説明
Is SRST Secure?	SRST 対応ゲートウェイに、自己署名証明書または認証局が発行した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。 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。 **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 Update をクリックし、従属する電話機をリセットします。
SRST Certificate Provider Port	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。 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。 **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い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。

表 7-2　SRST リファレンスのセキュリティ設定（続き）

設定	説明
Update SRST Certificate	**ヒント**　このボタンが表示されるのは、既存の SRST リファレンスのセキュリティ設定だけです。 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 証明書を置き換えます。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 証明書と共に）電話機に送信します。

関連項目

- SRST のセキュリティの概要（P.7-2）
- SRST のセキュリティ設定用チェックリスト（P.7-4）
- トラブルシューティング（P.9-1）