# セキュアな Survivable Remote Site Telephony（SRST）リファレンス

この章では、SRST リファレンスについて説明します。



## SRST セキュリティ

SRST 対応ゲートウェイは Unified Communications Manager がコールを完了できない場合に限定的な発信処理タスクを行います。

Secure 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。SRST 設定タスクを Unified Communications Manager Administrationで実行した後、 Unified Communications Manager はTLS接続を使用してSRST対応ゲートウェイで証明書プロバイダーサービスを認証します。Cisco Unified Communications Manager は次に SRST 対応ゲートウェイから証明書を取得し、この証明書を Unified Communications Manager データベースに追加します。

Unified Communications Manager Administration で従属デバイスをリセットすると、TFTP サーバは電話機の cnf.xml ファイルに SRST 対応ゲートウェイ証明書を追加し、そのファイルを電話機に送信します。その後、セキュアな電話は TLS 接続を使用して、SRST 対応ゲートウェイと相互に対話します。

**ヒント** 電話の設定ファイルには、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。

# SRST セキュリティのヒント

セキュアな電話と SRST 対応ゲートウェイ間の接続を保護するには、次の条件が満たされていることを確認してください。

- 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混合モードに設定している。
- 電話に認証または暗号化を設定している。
- SRST リファレンスを [Unified Communications Manager Administration] で設定している。
- SRST 設定後に SRST 対応ゲートウェイと従属する電話をリセットしている。

（注） Unified Communications Manager は、電話の証明書情報を含む PEM 形式のファイルを SRST 対応ゲートウェイに提供します。

（注） ロースピードラインカード（LSC）の認証の場合、CAPF のルート証明書（CAPF.der）をダウンロードします。このルート証明書によりセキュア SRST は TLS ハンドシェイク中に電話の LSC を確認できます。

- クラスタ セキュリティ モードが非セキュアの場合、[Unified Communications Manager 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であることが示されても、電話の設定ファイルではデバイスセキュリティ モードが非セキュアなままです。このような状況では、電話は SRST 対応ゲートウェイおよび Unified Communications Manager で非セキュアな接続を試みます。

  （注） クラスタ セキュリティ モードは、スタンドアロン サーバまたはクラスタのセキュリティ機能を設定します。

- クラスタ セキュリティ モードが非セキュアの場合、システムはセキュリティ関連の設定（デバイスのセキュリティ モード、[Is SRST Secure?] チェックボックスなど）を無視します。設定がデータベースから削除されることはありませんが、セキュリティは提供されません。
- 電話が SRST 対応ゲートウェイへのセキュアな接続を試行するのは、クラスタ セキュリティ モードが混合モードに設定されており、電話の設定ファイル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であり、[SRST Configuration] ウィンドウの [Is SRST Secure?] チェックボックスがオンになっており、有効な SRST 対応ゲートウェイの証明書が電話の設定ファイルにある場合だけです。

- 以前の Unified Communications Manager リリースでセキュア SRST リファレンスを設定していた場合、設定の移行はアップグレード中に自動的に行われます。
- 暗号化または認証済みモードの電話が SRST にフェールオーバーし、SRST での接続中に、クラスタ セキュリティ モードが混合モードから非セキュア モードに切り替わる場合、これらの電話は自動的に Unified Communications Manager にフォールバックしません。SRST ルータの電源をオフにし、これらの電話を Unified Communications Manager に強制的に再登録します。電話が Unified Communications Manager にフォールバックした後、SRST に電源を入れることができます。フェールオーバーとフォールバックは再び自動になります。

# セキュアな SRST の設定

次の手順は、SRST のセキュリティ設定手順を示します。

**手順**

**ステップ 1** デバイスが Unified Communications Manager とセキュリティに対応できるよう、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。

詳細は、このバージョンの Unified Communications Manager に対応した『*Cisco IOS SRST Version System Administrator Guide*』を参照してください。

**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。

**ステップ 3** 電話に証明書が存在することを確認します。

詳細は、ご使用の電話のモデルの Cisco Unified IP Phone ドキュメンテーションを参照してください。

**ステップ 4** 電話に認証または暗号化を設定したことを確認します。

**ステップ 5** SRST リファレンスのセキュリティ設定を行います。これには、[Device Pool Configuration] ウィンドウで SRST リファレンスを有効化することも含まれます。

**ステップ 6** SRST 対応ゲートウェイと電話をリセットします。

# セキュアな SRST リファレンスの設定

[Cisco Unified Communications Manager Administration][Unified Communications Manager 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。

- セキュアな SRST リファレンスの追加：初めて SRST リファレンスのセキュリティ設定を行う際に、表 1 : セキュア SRST リファレンスの設定 （6 ページ）で説明されているすべての項目を設定する必要があります。
- セキュアな SRST リファレンスの更新：[Unified Communications Manager 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は更新されません。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。このボタンをクリックすると、証明書の内容が表示されるので、この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、Unified Communications Manager では、Unified Communications Manager サーバ、またはクラスタ内の各 Unified Communications Manager サーバで、信頼できるフォルダ内にある SRST 対応ゲートウェイの証明書を置き換えます。
- セキュアな SRST リファレンスの削除：セキュアな SRST リファレンスを削除すると、Unified Communications Manager データベースおよび電話の 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 リファレンスの削除方法については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

セキュアな SRST リファレンスを設定するには、次の手順を実行します。

**手順**

**ステップ 1** [Unified Communications Manager Administration] で、**[System]** > **[SRST]** を選択します。

[Find and List] ウィンドウが表示されます。

**ステップ 2** 次のいずれかの作業を実行します。

a) 新しい SRST リファレンスを追加するには、[Find] ウィンドウで [Add New] をクリックします（プロファイルを表示してから、[Add New] をクリックすることもできます）。各フィールドにデフォルト設定が取り込まれた設定ウィンドウが表示されます。

b) 既存の SRST リファレンスをコピーするには、『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って適切な SRST リファレンスを見つけ、[Copy] 列内にあるそのレコード用の [Copy] アイコンをクリックします（プロファイルを表示してから、[Copy] をクリックすることもできます）。設定ウィンドウが表示され、設定された項目が示されます。

c) 既存の SRST リファレンスを更新するには、『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って適切な SRST リファレンスを見つけます。

設定ウィンドウが表示され、現在の設定が示されます。

**ステップ 3** 表 1 : セキュア SRST リファレンスの設定 （6 ページ）の説明に従ってセキュリティ関連の設定を入力します。

追加の SRST リファレンスの設定項目については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

[Find and List] ウィンドウが表示されます。

**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ことを示す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** [保存（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] をクリックした場合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。

### 次のタスク

[Device Pool Configuration] ウィンドウで SRST リファレンスを有効にしたことを確認します。

# SRST リファレンスのセキュリティ設定

次の表では、[Unified Communications Manager Administration] で利用可能なセキュア SRST リファレンスの設定を説明します。

表 *1:* セキュア *SRST* リファレンスの設定

| 設定 | 説明 |
|---|---|
| [Is SRST Secure?] | SRST対応ゲートウェイに自己署名証明書が含まれることを確認した後で、このチェックボックスをオンにします。<br><br>SRSTを設定してゲートウェイおよび従属する電話をリセットすると、Cisco CTL プロバイダー サービスは SRST 対応ゲートウェイで証明書プロバイダー サービスに対して認証します。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、この証明書を Unified Communications Manager データベースに保存します。<br><br>ヒント　SRST 証明書をデータベースおよび電話から削除するには、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 対応ゲートウェイで証明書プロバイダー サービスの要求をモニタします。Unified Communications Manager 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 証明書プロバイダーのデフォルト ポートは2445 です。<br><br>SRST対応ゲートウェイ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。<br><br>ヒント　ポートが現在使用されているか、またはファイアウォールを使用していてファイアウォール内でポートを使用できない場合、異なるポート番号を設定する必要があります。ポート番号は 1024～49151 の範囲内である必要があります。範囲外の場合には「Port Numbers can only contain digits」というメッセージが表示されます。 |

| 設定 | 説明 |
|---|---|
| [Update Certificate] | 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] をクリックした場合にだけ表示されます。<br><br>証明書がデータベースにある場合、このボタンをクリックすると、Cisco CTL クライアントが Unified Communications Manager データベースに保存されている 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）。従属する電話をリセットすると、TFTP サーバは cnf.xml ファイル（および新しい SRST 対応ゲートウェイ証明書）を送信します。 |

# SRST リファレンスからのセキュリティの削除

セキュリティ設定後に SRST リファレンスを非セキュアにするには、[SRST Configuration] ウィンドウの [Is SRTS Secure?] チェック ボックスをオフにします。ゲートウェイのクレデンシャル サービスを無効にする必要があることを示すメッセージが表示されます。

# ゲートウェイからの SRST 証明書の削除

SRST 証明書が SRST 対応ゲートウェイに存在しない場合は、Unified Communications Manager データベースおよび電話から、SRST 証明書を削除する必要があります。

この作業を実行するには、[SRST Secure?] チェック ボックスをオフにし、[SRST Configuration] ウィンドウで [Update] をクリックします。次に [Reset Decives] をクリックします。