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 電話機の設定ファイルには、1つの発行者からの証明書のみが含まれています。そのため、システムは HSRP をサポートしていません。

SRST のセキュリティのヒント

セキュアな電話機と SRST 対応ゲートウェイ間の接続を保護するために、次の基準が満たされていることを確認します。

- SRST リファレンスには、自己署名証明書が含まれています。
- Cisco CTL クライアントを使用して混合モードを設定しました。
- 認証または暗号化のために電話機を設定しました。
- 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） LSC 認証の場合は、CAPF 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機の 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と同等の場合、システムはセキュリティ関連の設定を無視します。たとえば、デバイスセキュリティモードの場合は SRST セキュアですか。チェックボックスなどをオンにします。設定はデータベースから削除されませんが、セキュリティは提供されません。
- 電話機は、クラスタセキュリティモードが混合モードになっている場合にのみ、SRST 対応ゲートウェイへのセキュアな接続を試行します。電話設定ファイルのデバイスセキュリティモードが authenticated または encrypted に設定されている場合は、SRST セキュアですか。[**Srst 設定 (Srst Configuration)**] ウィンドウでチェックボックスがオンになっており、有効な srst 対応ゲートウェイ証明書が電話機の設定ファイルに存在しています。

- 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、セキュリティのために SRST 設定プロセスを実行するタスクを示しています。

手順

Step 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『*CiscoIOS SRST Version System Administrator Guide*』を参照してください。

Step 2 CiscoCTL クライアントをインストールして設定するために必要なすべてのタスクを実行したことを確認します。

Step 3 電話に証明書が存在することを確認します。

詳細については、ご使用の電話機モデルのCisco Unified IP 電話 のマニュアルを参照してください。

Step 4 電話機が認証または暗号化用に設定されていることを確認します。

Step 5 [デバイスプールの設定 (Device Pool Configuration)] ウィンドウでの SRST リファレンスの有効化を含む、セキュリティのための SRST リファレンスを設定します。

Step 6 SRST 対応のゲートウェイと電話をリセットします。

関連トピック

電話機へのセキュリティ プロファイルの適用
Cisco CTL クライアントの設定
セキュア SRST リファレンスのセットアップ, on page 4

セキュア SRST リファレンスのセットアップ

[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

Step 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。

Step 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、**[新規追加 (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] 列でそのレコードの [**copy**] アイコンをクリックします。(プロファイルを表示し、**[コピー (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。

Step 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。

SRST リファレンスの追加設定の詳細については、 *Cisco Unified Communications Manager* のアドミニストレーションガイドを参照してください。

[Find and List] ウィンドウが表示されます。

Step 4 [Is SRST Secure?] をオンにした後、チェックボックスをオンにすると、[証明書の更新 (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。

Step 5 [保存（Save）] をクリックします。

Step 6 データベース内の SRST 対応ゲートウェイ証明書を更新するには、[**証明書の更新 (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。

Step 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。

Step 8 [閉じる（Close）] をクリックします。

Step 9 [SRST Reference Configuration] ウィンドウで、[**Reset**] をクリックします。

次のタスク

[**デバイスプールの設定 (Device Pool Configuration)**] ウィンドウで srst リファレンスが有効になっていることを確認します。

関連トピック

SRST セキュリティに関する詳細情報の入手先

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
セキュアSRST（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。 SRST を設定し、ゲートウェイおよび従属する電話をリセットすると、CiscoCTL Provider サービスは、SRST 対応のゲートウェイ上の証明書プロバイダサービスに対して認証を行います。CiscoCTL 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。 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 証明書 プロバイダー ポート（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。CiscoSRST 証明書プロバイダのデフォルトポートは 2445 です。 SRST 対応のゲートウェイ上でこのポートを設定したら、このフィールドにポート番号を入力します。 ヒント　ポートが現在使用されている場合、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のポートを使用できない場合は、別の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 の範囲内に存在する必要があります。それ以外の場合は、次のメッセージが表示されます: ポート番号には数字のみを含めることができます。

設定	説明
証明書を更新する（Update Certificate）	ヒント　このボタンは、[セキュア SRST（Is SRST Secure?）] チェックボックスをオンにして [保存（Save）] をクリックした場合のみ表示されます。 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、CiscoCTL 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 対応のゲートウェイ証明書）を電話に送信します。

関連トピック

SRST のセキュリティのヒント, on page 2
詳細情報の入手先

SRST リファレンスからのセキュリティの削除

セキュリティを設定した後に SRST リファレンスを非セキュアにするには、[Is SRST Secure?] チェックボックスをオフにします。[SRST 設定 (SRST Configuration)] ウィンドウのチェックボックスをオンにします。ゲートウェイのクレデンシャルサービスをオフ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。

このタスクを実行するには、[**IS Srst Secure?**] チェックボックスをオフにして、[Srst Configuration] ウィンドウで [**Update**] をクリックします。次に、[**Reset Devices**] をクリックします。