CHAPTER 13

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 Unified Communications Manager 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 Unified Communications Manager の管理ページで SRST 設定作業を実行した後、Cisco 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 サービスを認証します。Cisco Unified Communications Manager 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 Unified Communications Manager データベースに追加します。

Cisco Unified Communications Manager の管理ページ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。

SRST セキュリティの設定のヒント

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接続の安全が保障されます。

- 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混合モードを設定した。
- 電話機に認証または暗号化を設定した。
- Cisco Unified Communications Manager の管理ページで 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。

（注）　Cisco Unified Communications Manager は、SRST 対応ゲートウェイ向けに、電話機の証明書情報を含む PEM 形式のファイルを提供します。

LSC 認証では、CAPF ルート証明書（CAPF.der）をダウンロードしてください。このルート証明書では、セキュアな SRST が 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になっている場合は、Cisco Unified Communications Manager の管理ページでデバイス 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 モードは非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 Unified Communications Manager サーバとの非セキュア接続を試行します。
- クラスタ セキュリティ モードが非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［セキュア SRST(Is SRST Secure?)］チェックボックスなど、セキュリティ関連の設定が無視されます。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 モードが混合モードで、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 参照先の設定 (SRST Reference Configuration)］ウィンドウで［セキュア SRST(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。
- 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 Unified Communications Manager セキュリティ モードが混合モードから非セキュア モードに切り替わった場合、これらの電話機は自動的には Cisco Unified Communications Manager にフォールバックされません。SRST ルータの電源を切り、強制的にこれらの電話機を Cisco Unified Communications Manager に再登録する必要があります。電話機が Cisco Unified Communications Manager 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 13-1 を使用して、SRST のセキュリティ設定手順を進めます。

表 13-1　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 Unified Communications Manager 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 Unified Communications Manager をサポートする『*Cisco IOS SRST Version 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 Unified 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。	電話機セキュリティ プロファイルの適用（P.5-12）
ステップ 5	SRST リファレンスにセキュリティを設定します。これには、［デバイスプール設定 (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.13-4）
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.13-4）

SRST リファレンスのセキュリティ設定

Cisco Unified Communications Manager の管理ページで 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 13-2 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 Unified Communications Manager の管理ページで 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、［証明書の更新］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 Unified Communications Manager は Cisco Unified Communications Manager サーバまたはクラスタ内の各 Cisco Unified Communications Manager 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 Unified Communications Manager 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 リファレンスの削除方法は、『*Cisco Unified Communications Manager 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 Unified Communications Manager の管理ページで、［**システム**］> **[SRST]** を選択します。

検索と一覧表示ウィンドウが表示されます。

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、検索ウィンドウで［**新規追加**］ボタンまたは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、［**新規追加**］ボタンまたはアイコン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、各フィールドのデフォルト設定が示されます。
- 既存の SRST リファレンスをコピーするには、『*Cisco Unified Communications Manager 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 (Copy)］列内にあるそのレコード用の［**コピー (Copy)**］ボタンをクリックします（プロファイルを表示してから、［**コピー**］ボタンまたはアイコン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、設定内容が示されます。
- 既存の SRST リファレンスを更新するには、『*Cisco Unified Communications Manager 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 13-2 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 Unified Communications Manager 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　［セキュア SRST(Is SRST Secure?)］チェックボックスをオンにすると、［証明書の更新］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　［**保存**］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、**［証明書の更新］**ボタンをクリックします。

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］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、**[保存]**をクリックします。

ステップ 8　**［閉じる］**をクリックします。

ステップ 9　［SRST 参照先の設定 (SRST Reference Configuration)］ウィンドウで、**[リセット]**をクリックします。

追加の手順

［デバイスプール設定 (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.13-7 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 13-2 で、保護された SRST リファレンスに対して Cisco Unified Communications Manager の管理ページで使用できる設定について説明します。

- 設定のヒントについては、P.13-2 の「SRST セキュリティの設定のヒント」を参照してください。
- 関連する情報および手順については、P.13-7 の「関連項目」を参照してください。

表 13-2　SRST リファレンスのセキュリティの設定内容

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、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証明書プロバイダ 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 Unified Communications Manager 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［保存］をクリックし、従属する電話機をリセットします。
［SRST 証明書プロバイダ ポート (SRST Certificate Provider Port)］	このポートは、SRST 対応ゲートウェイ上で証明書プロバイダ サービスに対する要求を監視します。Cisco 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。ポート番号は、1024 ～ 49151 の範囲に存在する必要があります。この範囲外にある場合、「ポート番号に使用できるのは数字だけです。」というメッセージが表示されます。
［証明書の更新］	**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］をクリックした後にだけ表示されます。 このボタンをクリックすると、Cisco CTL クライアントは Cisco Unified Communications Manager 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。

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 リファレンスを非セキュアにするには、［SRST 参照先の設定 (SRST Reference Configuration)］ウィンドウで、［セキュア SRST(Is SRST 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 証明書がゲートウェイから削除された場合

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 Unified Communications Manager 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 参照先の設定 (SRST Reference Configuration)］ウィンドウで、**［セキュア SRST(Is SRST Secure?)］**チェックボックスをオフにして **［保存］**をクリックし、**［リセット］**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.13-1）
- SRST セキュリティの設定のヒント（P.13-2）
- SRST のセキュリティ設定用チェックリスト（P.13-3）
- SRST リファレンスのセキュリティ設定（P.13-4）
- SRST リファレンスのセキュリティの設定内容（P.13-6）
- SRST リファレンスからのセキュリティの削除（P.13-7）
- SRST 証明書がゲートウェイから削除された場合（P.13-7）

シスコの関連マニュアル

- *Cisco IOS SRST System Administrator Guide*
- *Cisco Unified Communications Manager アドミニストレーション ガイド*