



セキュア SRST (Survivable Remote Site Telephony) 参照先の設定

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.22-1)
- 「SRST のセキュリティ設定のヒント」 (P.22-2)
- 「SRST のセキュリティ設定用チェックリスト」 (P.22-3)
- 「セキュア SRST 参照先の設定」 (P.22-3)
- 「SRST 参照先のセキュリティの設定内容」 (P.22-5)
- 「SRST 参照先からのセキュリティの解除」 (P.22-5)
- 「SRST 証明書がゲートウェイから削除された場合」 (P.22-6)
- 「参考情報」 (P.22-6)

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。

セキュア 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ー 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 のセキュリティ設定のヒント

次の基準が満たされていることを確認します。これらが満たされていると、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確保されます。

- SRST 参照先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 の管理で SRST 参照先を設定した。
- 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 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。



(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。
- 前のリリースの Cisco Unified Communications Manager でセキュア SRST 参照先を設定した場合は、アップグレード時にその設定が自動的に移行されます。
- 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 モードに切り替わった場合、これらの電話機は自動的に 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 22-1 を使用して、SRST のセキュリティ設定手順を進めます。

表 22-1 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 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.4-1)
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.7-11)
ステップ 5 SRST 参照先のセキュリティ設定を行います。これには、[デバイスプール設定(Device Pool Configuration)] ウィンドウで SRST 参照先を有効にする作業も含まれます。	「セキュア SRST 参照先の設定」(P.22-3)
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。	「セキュア SRST 参照先の設定」(P.22-3)

セキュア SRST 参照先の設定

Cisco Unified Communications Manager の管理で SRST 参照先を追加、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 SRST 参照先の追加：初めて SRST 参照先のセキュリティ設定を行う場合、表 22-2 で説明するすべての項目を設定する必要があります。
- セキュア SRST 参照先の更新：Cisco Unified Communications Manager の管理で 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(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 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。
- セキュア SRST 参照先の削除：セキュア SRST 参照先を削除すると、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 参照先の削除方法は、『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。

セキュア SRST 参照先を設定するには、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 (System)] > [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** 次のいずれかを実行します。
- 新しい SRST 参照先を追加するには、検索ウィンドウで [新規追加 (Add New)] 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 (Add New)] 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 参照先をコピーするには、『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 参照先を見つけ、[コピー (Copy)] 列内にあるそのレコード用の [コピー (Copy)] 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、[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、設定内容が示されます。
 - 既存の SRST 参照先を更新するには、『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 参照先を見つけます。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 22-2 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 参照先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 (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** [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、[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、[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 (Save)] をクリックします。
- ステップ 8** [閉じる (Close)] 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 (Reset)] をクリックします。

次の作業

[デバイスプール設定 (Device Pool Configuration)] ウィンドウで SRST 参照先が有効になったことを確認します。

追加情報

「関連項目」(P.22-6) を参照してください。

SRST 参照先のセキュリティの設定内容

表 22-2 で、セキュア SRST 参照先に対して Cisco Unified Communications Manager の管理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、「SRST のセキュリティ設定のヒント」(P.22-2) 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、「関連項目」(P.22-6) を参照してください。

表 22-2 セキュア SRST 参照先の設定内容

設定	説明
[セキュア SRST (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証明書プロバイダー 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。</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 [保存(Save)] をクリックし、従属する電話機をリセットします。</p>
[SRST 証明書プロバイダーポート (SRST Certificate Provider Port)]	<p>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ー 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 証明書プロバイダーのデフォルト 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>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。</p>
[証明書の更新 (Update Certificate)]	<p>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 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ともに) 電話機に送信します。</p>

SRST 参照先からのセキュリティの解除

セキュリティ設定後に SRST 参照先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た場合は、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 [更新 (Update)] をクリックし、[複数のデバイスのリセット (Reset Devices)] をクリックします。

参考情報

関連項目

- 「SRST のセキュリティの概要」 (P.22-1)
- 「SRST のセキュリティ設定のヒント」 (P.22-2)
- 「SRST のセキュリティ設定用チェックリスト」 (P.22-3)
- 「セキュア SRST 参照先の設定」 (P.22-3)
- 「SRST 参照先のセキュリティの設定内容」 (P.22-5)
- 「SRST 参照先からのセキュリティの解除」 (P.22-5)
- 「SRST 証明書がゲートウェイから削除された場合」 (P.22-6)

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』