CHAPTER 18

Cisco Unity Connection Survivable Remote Site Voicemail 9.1(1) での接続のセキュリティ保護

この章では、中央の Connection と Connection SRSV の間の通信をセキュリティで保護する方法について説明します。また、Cisco Unity Connection SRSV の管理と Connection SRSV の間の通信をセキュリティで保護する方法についても説明します。

次の項を参照してください。

- 「自己署名証明書に基づいたアクセスの使用」（P.18-1）
- 「中央の Connection サーバと Connection SRSV の間の接続の保護」（P.18-2）
- 「Connection SRSV の管理と Connection SRSV の間の接続の保護」（P.18-2）
- 「Microsoft 証明書サービスのインストール（Windows Server 2003 の場合のみ）」（P.18-5）
- 「ルート証明書のエクスポートとサーバ証明書の発行（Microsoft 証明書サービスの場合のみ）」（P.18-6）

自己署名証明書に基づいたアクセスの使用

中央の Connection サーバと Connection SRSV の間の通信に自己署名証明書に基づいたアクセスを使用できます。デフォルトでは、中央の Connection サーバと Connection SRSV は自己署名証明書を受け入れません。中央の Connection サーバと Connection SRSV で自己署名証明書を受け入れるには、管理者クレデンシャルを使用して、コマンド プロンプトで次の手順を実行する必要があります。

ステップ 1 次のコマンドを実行します。

```
run cuc dbquery unitydirdb EXECUTE PROCEDURE
csp_ConfigurationModify(pFullName='System.SRSV.AcceptSrsvSelfSignedCertificates',
pValue='1')
```

ステップ 2 次のコマンドを実行して、[System.SRSV.AcceptSrsvSelfSignedCertificates] フィールドの値が 1 に設定されていることを確認します。

```
run cuc dbquery unitydirdb select objectid,fullname,value from vw_configuration
where fullname like '%SRSV%'
```

[System.SRSV.AcceptSrsvSelfSignedCertificates] の値を 1 に変更したら、Connection Branch Sync Service および Tomcat サービスを再起動して、変更を反映し、自己署名証明書アクセスを許可する必要があります。

Tomcat サービスを再起動するには、次の手順を実行します。

ステップ 1　SSH アプリケーションを使用して Connection サーバにサインインします。

ステップ 2　次の CLI コマンドを使用して Tomcat サービスを再起動します。

```
utils service restart Cisco Tomcat
```

中央の Connection サーバと Connection SRSV の間の接続の保護

Connection SRSV は、セキュア ソケット レイヤ（SSL）と共有秘密の両方を使用して、中央の Connection とブランチ間の通信をセキュリティで保護します。

1. SSL 証明書のインストール

Cisco Unity Connection SRSV をインストールすると、ローカル証明書が自動的に作成され、Connection SRSV と Connection の間の通信をセキュリティで保護するためにインストールされます。つまり、Connection SRSV と Connection の間のすべてのネットワーク トラフィック（ユーザ名、パスワード、その他のテキスト データ、およびボイス メッセージを含む）が自動的に暗号化されます。SSL 証明書のインストールの詳細については、『*Security Guide for Cisco Unity Connection*』*Release 9.x* の「Using SSL to Secure Client/Server Connections in Cisco Unity Connection 9.x」の章を参照してください。このドキュメントは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/security/guide/9xcucsecx.html から入手可能です。

2. 共有秘密の使用

Connection SRSV は共有秘密を使用して、Connection のアクセスを認証します。共有秘密の詳細については、『*Security Guide for Cisco Unity Connection*』*Release 9.x* の「Passwords, PINs, and Authentication Rule Management in Cisco Unity Connection 9.x」の章の「Cisco Unity Connection SRSV Passwords and Shared Secrets」を参照してください。このドキュメントは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/security/guide/9xcucsecx.html から入手可能です。

Connection SRSV の管理と Connection SRSV の間の接続の保護

Connection SRSV への Connection SRSV の管理のアクセスをセキュリティで保護するためには、次のタスクを実行して、SSL サーバ証明書を作成してインストールする必要があります。

1. Microsoft 証明書サービスを使用して証明書を発行する場合は、Microsoft 証明書サービスをインストールします。Windows Server 2003 を実行しているサーバに Microsoft 証明書サービスをインストールする方法については、「Microsoft 証明書サービスのインストール（Windows Server 2003 の場合のみ）」（P.18-5）を参照してください。それ以降のバージョンの Windows Server を実行しているサーバに Microsoft 証明書サービスをインストールする方法については、Microsoft 社のドキュメントを参照してください。

   別のアプリケーションを使用して証明書を発行する場合は、そのアプリケーションをインストールします。インストールの方法については、製造元が提供しているドキュメントを参照してください。その後で、タスク 2 に進みます。

外部の認証局を使用して証明書を発行する場合は、タスク 2 に進みます。

（注）　Microsoft 証明書サービス、または証明書署名要求を作成できる別のアプリケーションをすでにインストールしてある場合は、タスク 2 に進みます。

2. 証明書署名要求を作成します。その後で、Microsoft 証明書サービスまたは証明書を発行するその他のアプリケーションをインストールしたサーバに証明書署名要求をダウンロードするか、証明書署名要求を外部の CA に送る際に使用するサーバに要求をダウンロードします。「証明書署名要求を作成およびダウンロードするには」（P.18-3）の手順を行います。
3. Microsoft 証明書サービスを使用してルート証明書のエクスポートおよびサーバ証明書の発行を行う場合は、「ルート証明書のエクスポートとサーバ証明書の発行（Microsoft 証明書サービスの場合のみ）」（P.18-6）の手順を実行します。

   証明書の発行に別のアプリケーションを使用する場合は、証明書の発行についてアプリケーションの資料を参照してください。

   証明書の発行に外部の CA を使用する場合は、外部の CA に証明書署名要求を送信します。外部 CA から証明書が返されたら、タスク 4 に進みます。

   Connection SRSV にアップロードできるのは、PEM 形式（Base-64 エンコードされた DER）の証明書だけです。証明書のファイル名拡張子は .pem であることが必要です。証明書がこの形式でない場合、通常は、OpenSSL など、無償で使用できるユーティリティを使用して PEM 形式に変換できます。
4. ルート証明書とサーバ証明書を Connection SRSV サーバにアップロードします。「ルート証明書とサーバ証明書を Cisco Unity Connection SRSV サーバにアップロードするには」（P.18-4）の手順を行います。
5. ユーザが Connection SRSV の管理または Connection を使用して Connection SRSV にアクセスするたびにセキュリティ警告が表示されないようにするには、ユーザが Connection SRSV へのアクセスを行うすべてのコンピュータ上で、次のタスクを実行します。
   - タスク 4 で Connection SRSV サーバにアップロードしたサーバ証明書を証明書ストアにインポートします。手順はブラウザによって異なります。詳細については、ブラウザのマニュアルを参照してください。
   - タスク 4 で Connection SRSV サーバにアップロードしたサーバ証明書を Java ストアにインポートします。手順は、クライアント コンピュータ上で実行されているオペレーティング システムによって異なります。詳細については、オペレーティング システムのドキュメントおよび Java ランタイム環境のドキュメントを参照してください。

証明書署名要求を作成およびダウンロードするには

ステップ 1　Cisco Unity Connection SRSV サーバで Cisco Unified オペレーティング システムの管理にサインインします。

ステップ 2　[セキュリティ（Security）] メニューで [証明書の管理（Certificate Management）] を選択します。

ステップ 3　[証明書の一覧（Certificate List）] ページで、[CSRCritical Services の作成（Generate CSR）] を選択します。

ステップ 4　[証明書署名要求の作成（Generate Certificate Signing Request）] ページの [証明書の名前（Certificate Name）] リストで、[tomcat] を選択します。

ステップ 5　[CSR の作成（Generate CSR）] を選択します。

ステップ 6　CSR が正常に生成されたことを示すメッセージがステータス エリアに表示されたら、[閉じる（Close）] を選択します。

ステップ 7　[証明書の一覧（Certificate List）] ページで、[CSR のダウンロード（Download CSR）] を選択します。

ステップ 8　[証明書署名要求のダウンロード（Download Certificate Signing Request）] ページの [証明書の名前（Certificate Name）] リストで、[tomcat] を選択します。

ステップ 9　[CSR のダウンロード（Download CSR）] を選択します。

ステップ 10　[ファイルのダウンロード（File Download）] ダイアログボックスで、[保存（Save）] を選択します。

ステップ 11　[名前を付けて保存（Save As）] ダイアログボックスの [保存の種類（Save As Type）] リストで、[すべてのファイル（All Files）] を選択します。

ステップ 12　**tomcat.csr** ファイルを、Microsoft 証明書サービスをインストールしたサーバ、または外部の認証局に CSR を送信するのに使用できるサーバ上の場所に保存します。

ステップ 13　[証明書署名要求のダウンロード（Download Certificate Signing Request）] ページで、[閉じる（Close）] を選択します。

ルート証明書とサーバ証明書を Cisco Unity Connection SRSV サーバにアップロードするには

ステップ 1　証明書署名要求を作成した Cisco Unity Connection SRSV サーバで、Cisco Unified Operating System の管理にサインインします。

ステップ 2　[セキュリティ（Security）] メニューで [証明書の管理（Certificate Management）] を選択します。

（注）　[検索（Find）] を選択し、現在そのサーバにインストールされている証明書のリストを表示すると、既存の、自動的に生成された、Tomcat の自己署名証明書が表示されます。この証明書は、この手順でアップロードする Tomcat 証明書とは関係のないものです。

ステップ 3　ルート証明書をアップロードします。

a.　[証明書の一覧（Certificate List）] ページで、[証明書のアップロード（Upload Certificate）] を選択します。

b.　[証明書のアップロード（Upload Certificate）] ページの [証明書の名前（Certificate Name）] リストで、[tomcat-trust] を選択します。

c.　[ルート証明書（Root Certificate）] フィールドは空白のままにします。

d.　[参照（Browse）] を選択して、ルート CA 証明書の場所を参照します。

証明書の発行に Microsoft 証明書サービスを使用した場合は、「ルート証明書をエクスポートし、サーバ証明書を発行するには」（P.18-7）の手順でエクスポートしたルート証明書がこの場所に保存されます。

証明書の発行に外部の認証局を使用した場合は、外部の認証局から受け取ったルート CA 証明書がこの場所に保存されます。

e.　ファイルの名前を選択します。

f.　[開く（Open）] を選択します。

g.　[証明書のアップロード（Upload Certificate）] ページで、[ファイルのアップロード（Upload File）] を選択します。

h.　アップロードに成功したことを示すメッセージがステータス エリアに表示されたら、[閉じる（Close）] を選択します。

ステップ 4　サーバ証明書をアップロードします。

a. [証明書の一覧（Certificate List）] ページで、[証明書のアップロード（Upload Certificate）] を選択します。

b. [証明書のアップロード（Upload Certificate）] ページの [証明書の名前（Certificate Name）] リストで、[tomcat] を選択します。

c. [ルート証明書（Root Certificate）] フィールドに、ステップ 3 でアップロードしたルート証明書のファイル名を入力します。

d. [参照（Browse）] を選択して、サーバ証明書の場所を参照します。

証明書の発行に Microsoft 証明書サービスを使用した場合は、「ルート証明書をエクスポートし、サーバ証明書を発行するには」（P.18-7）の手順で発行したサーバ証明書がこの場所に保存されます。

証明書の発行に外部の認証局を使用した場合は、外部の認証局から受け取ったサーバ証明書がこの場所に保存されます。

e. ファイルの名前を選択します。

f. [開く（Open）] を選択します。

g. [証明書のアップロード（Upload Certificate）] ページで、[ファイルのアップロード（Upload File）] を選択します。

h. アップロードに成功したことを示すメッセージがステータス エリアに表示されたら、[閉じる（Close）] を選択します。

ステップ 5　Tomcat サービスを再起動します（このサービスは Cisco Unified Serviceability からは再起動できません）。

a. SSH アプリケーションを使用して Cisco Unity Connection SRSV サーバにサインインします。

b. 次の CLI コマンドを使用して Tomcat サービスを再起動します。

```
utils service restart Cisco Tomcat
```

Connection Branch Sync Service の再起動方法

ステップ 1　Cisco Unity Connection Serviceability にログインします。

ステップ 2　[ツール（Tools）] メニューで [サービス管理（Service Management）] を選択します。

ステップ 3　[オプション サービス（Optional Services）] セクションで、Connection Branch Sync Service の [停止（Stop）] を選択します。

ステップ 4　Connection IMAP サーバ サービスが正常に停止したことを示すメッセージがステータス エリアに表示されたら、このサービスに [開始（Start）] を選択します。

Microsoft 証明書サービスのインストール（Windows Server 2003 の場合のみ）

サードパーティの認証局を使用して SSL 証明書を発行する場合や、Microsoft 証明書サービスがすでにインストールされている場合は、この項の手順を省略してください。

Microsoft 証明書サービスを使用して独自の証明書を発行する場合で、Windows Server 2003 を実行しているサーバにこのアプリケーションをインストールする場合に、この項の手順を実行します。

ルート認証局（Microsoft 証明書サービスの一般的な名称）を Windows Server 2008 サーバにインストールする場合は、Windows Server 2008 のオンライン ヘルプを参照してください。

Microsoft 証明書サービス コンポーネントをインストールするには

ステップ 1　Connection SRSV ボイス メッセージにアクセスするすべてのクライアント コンピュータで解決できる DNS 名（FQDN）または IP アドレスを持つサーバ上で、ローカル Administrators グループのメンバーであるアカウントを使用して Windows にログインします。

ステップ 2　Windows の [スタート（Start）] メニューで、[設定（Settings）] > [コントロール パネル（Control Panel）] > [プログラムの追加と削除（Add or Remove Programs）] を選択します。

ステップ 3　[プログラムの追加と削除（Add or Remove Programs）] の左側のパネルで、[Windows コンポーネントの追加と削除（Add/Remove Windows Components）] を選択します。

ステップ 4　[Windows コンポーネント（Windows Components）] ダイアログボックスで、[証明書サービス（Certificate Services）] チェックボックスをオンにします。他の項目は変更しないでください。

ステップ 5　コンピュータ名の変更やドメイン メンバーシップの変更ができないことを通知する警告が表示されたら、[はい（Yes）] を選択します。

ステップ 6　[次へ（Next）] を選択します。

ステップ 7　[CA の種類（CA Type）] ページで、[スタンドアロンのルート CA（Stand-alone Root CA）] を選択し、[次へ（Next）] を選択します。（スタンドアロンの認証局（CA）とは、Active Directory を必要としない CA です）。

ステップ 8　[CA の ID 情報（CA Identifying Information）] ページの [この CA の通常名（Common Name for This CA）] フィールドに、認証局の名前を入力します。

ステップ 9　[識別名サフィックス（Distinguished Name Suffix）] フィールドで、デフォルトの値を受け入れます。

ステップ 10　有効期間として、デフォルト値の [5 年（5 Years）] を受け入れます。

ステップ 11　[次へ（Next）] を選択します。

ステップ 12　[証明書データベース設定（Certificate Database Settings）] ページで、[次へ（Next）] を選択してデフォルト値を受け入れます。

インターネット インフォメーション サービスがコンピュータ上で実行されており、先に進むにはこのサービスを停止する必要があることを通知するメッセージが表示されたら、[はい（Yes）] を選択してこのサービスを停止します。

ステップ 13　Windows Server 2003 のディスクをドライブに挿入するように求められたら、そのように実行します。

ステップ 14　[Windows コンポーネントの完了ウィザード（Completing the Windows Components Wizard）] ダイアログボックスで、[終了（Finish）] を選択します。

ステップ 15　[プログラムの追加と削除（Add or Remove Programs）] ダイアログボックスを閉じます。

ルート証明書のエクスポートとサーバ証明書の発行（Microsoft 証明書サービスの場合のみ）

Microsoft 証明書サービスを使用して証明書を発行する場合だけ、次の手順を実行します。

ルート証明書をエクスポートし、サーバ証明書を発行するには

ステップ 1　Microsoft 証明書サービスをインストールしたサーバで、Domain Admins グループのメンバであるアカウントを使用して Windows にサインインします。

ステップ 2　Windows の [スタート（Start）] メニューで、[プログラム（Programs）] > [管理ツール（Administrative Tools）] > [証明機関（Certification Authority）] を選択します。

ステップ 3　左側のパネルで、[認証局（ローカル）（Certification Authority (Local)）] > <認証局の名前> を展開します。<認証局の名前> は、「Microsoft 証明書サービス コンポーネントをインストールするには」（P.18-6）の手順で Microsoft 証明書サービスをインストールしたときに認証局に付けた名前になります。

ステップ 4　ルート証明書をエクスポートします。

a. 認証局の名前を右クリックし、[プロパティ（Properties）] を選択します。

b. [全般（General）] タブで、[証明書の表示（View Certificate）] を選択します。

c. [詳細（Details）] タブを選択します。

d. [ファイルのコピー（Copy to File）] を選択します。

e. [証明書のエクスポート ウィザードの開始（Welcome to the Certificate Export Wizard）] ページで、[次へ（Next）] を選択します。

f. [エクスポート ファイルの形式（Export File Format）] ページで [次へ（Next）] をクリックして、デフォルト値 [DER Encoded Binary X.509 (.CER)] を受け入れます。

g. [エクスポートするファイル（File to Export）] ページで、.cer ファイルのパスとファイル名を入力します。Connection サーバからアクセス可能なネットワーク上の場所を選択します。

パスとファイル名を書き留めます。この情報は後の手順で必要になります。

h. ウィザードでエクスポートが完了するまで、画面に表示される指示に従って操作します。

i. [OK] を選択して [証明書（Certificate）] ダイアログボックスを閉じ、もう一度 [OK] を選択して [プロパティ（Properties）] ダイアログボックスを閉じます。

ステップ 5　サーバ証明書を発行します。

a. 認証局の名前を右クリックし、[すべてのタスク（All Tasks）] > [新しい要求の送信（Submit New Request）] を選択します。

b. 「証明書署名要求を作成およびダウンロードするには」（P.18-3）の手順 で作成した証明書署名要求ファイルの場所に移動し、このファイルをダブルクリックします。

c. [認証局（Certification Authority）] の左側のパネルで [保留中の要求（Pending Requests）] を選択します。

d. b. で送信した保留中の要求を右クリックし、[すべてのタスク（All Tasks）] > [発行（Issue）] を選択します。

e. [認証局（Certification Authority）] の左側のパネルで [発行済み証明書（Issued Certificates）] を選択します。

f. 新しい証明書を右クリックし、[すべてのタスク（All Tasks）] > [バイナリ データのエクスポート（Export Binary Data）] を選択します。

g. [バイナリ データのエクスポート（Export Binary Data）] ダイアログボックスの [バイナリ データが含まれている列（Columns that Contain Binary Data）] リストで、[バイナリ証明書（Binary Certificate）] を選択します。

h. [バイナリ データをファイルに保存（Save Binary Data to a File）] を選択します。

i. [OK] を選択します。

j. [バイナリ データの保存（Save Binary Data）] ダイアログボックスで、パスとファイル名を入力します。Connection SRSV サーバからアクセス可能なネットワーク上の場所を選択します。

パスとファイル名を書き留めます。この情報は後の手順で必要になります。

k. [OK] を選択します。

ステップ 6　[認証局（Certification Authority）] を閉じます。