Microsoft Office Communications Server for Partitioned Intradomain Federation の設定

（注） この章の手順は、Microsoft Office Communications Server (OCS) 2007 R2 にのみ適用されます。

OCS サーバでポート 5060 を有効にする

IM and Presence および OCS 間の SIP トラフィックについて暗号化されていない TCP 接続を使用する場合、TCP SIP ポート 5060 をリッスンするよう OCS を設定する必要があります。 次の手順では、OCS サーバでポート 5060 を有効にする方法について説明します。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンド サーバでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 Standard Edition または Enterprise Edition フロントエンド サーバの FQDN を右クリックし、[プロパティ（Properties）] > [フロントエンドのプロパティ（Front End Properties）] を選択します。

ステップ 3 [全般（General）] タブをクリックします。

ステップ 4 [接続（Connections）] にポート 5060 が記載されていない場合は、[追加（Add）] を選択します。

ステップ 5 [IP アドレス（IP Address）] 値に **All** を選択します。

ステップ 6 [ポート（Port）] 値に **5060** を選択します。

ステップ 7 [トランスポート（Transport）] 値に **TCP** を選択します。

ステップ 8 [OK] をクリックして、[接続の追加（Add Connection）] ウィンドウを閉じます。 これで、ポート 5060 が [接続（Connections）] リストに記載されているはずです。

ステップ 9 [OK] を再度選択して、[フロントエンド サーバ プロパティ（Front End Server Properties）] ウィンドウを閉じます。

次の作業

IM and Presence をポイントするよう OCS スタティック ルートを設定する，（2 ページ）

関連トピック

統合のトラブルシューティング

IM and Presence をポイントするよう OCS スタティック ルートを設定する

OCS が要求を IM and Presence にルーティングできるようにするには、OCS サーバでスタティック ルートを設定する必要があります。 スタティック ルートは IM and Presence をポイントします。 次の手順は、必要なスタティック ルートを設定する方法を説明します。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのプールでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 適宜 Enterprise Edition プール名または Standard Edition サーバ名を右クリックします。

ステップ 3 [プロパティ（Properties）]>[フロントエンドのプロパティ（Front End Properties）] を選択します。

ステップ 4 [ルーティング（Routing）] タブを選択し、[追加（Add）] を選択します。

ステップ 5 foo.com など、IM and Presence サーバのドメインを入力します。

ステップ 6 [電話の URI（Phone URI）] チェックボックスがオフになっていることを確認します。

ステップ 7 IM and Presence サーバの IP アドレスをネクスト ホップの IP アドレスとして入力します。

ステップ 8 [ネクスト ホップ トランスポート（Next Hop Transport）] 値に **TCP** を選択します。

ステップ 9 [ネクスト ホップ ポート（Next Hop Port）] 値に **5060** を入力します。

ステップ 10 [要求 URI 内のホストを置き換える（Replace host in request URI）] チェックボックスがオフになっていることを確認します。

ステップ 11 [OK] をクリックして、[静的ルートの追加（Add Static Route）] ウィンドウを閉じます。 新しいスタティック ルートがルーティング リストに表示されるはずです。

ステップ 12 [OK] を再度選択して、[フロントエンド サーバ プロパティ（Front End Server Properties）] ウィンドウを閉じます。

次の作業

IM and Presence の OCS でのホスト認証の追加, （3 ページ）

関連トピック

統合のトラブルシューティング

IM and Presence の OCS でのホスト認証の追加

認証を求められずに OCS が IM and Presence から SIP 要求を承認できるようにするには、IM and Presence サーバごとに OCS でホスト認証エントリを設定する必要があります。

OCS および IM and Presence 間の TLS 暗号化を設定している場合、次のように IM and Presence サーバごとに 2 つのホスト認証エントリを追加する必要があります。

- 最初のエントリには、IM and Presence サーバの FQDN が含まれている必要があります。
- 2 つ目のエントリには、IM and Presence サーバの IP アドレスが含まれている必要があります。

TLS 暗号化を設定していない場合、IM and Presence サーバごとにホスト認証エントリを 1 つだけ追加します。 このホスト認証エントリには、IM and Presence サーバの IP アドレスが含まれている必要があります。

次の手順では、必要なホスト認証エントリを追加する方法について説明します。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのプールでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 適宜 Enterprise Edition プール名または Standard Edition サーバ名を右クリックします。

ステップ 3 [プロパティ（Properties）] > [フロントエンドのプロパティ（Front End Properties）] を選択します。

ステップ 4 [ホストの承認（Host Authorization）] タブを選択して、[追加（Add）] を選択します。

ステップ 5 FQDN を入力している場合、[FQDN] を選択して、IM and Presence サーバの FQDN を入力します。たとえば、cup1.foo.com などです。

ステップ 6 IP アドレスを入力する場合は、[IP アドレス（IP Address）] を選択し、IM and Presence サーバの IP アドレスを入力します。 たとえば、10.x.x.x などです。

ステップ 7 [送信のみ（Outbound Only）] チェックボックスがオフになっていることを確認します。

ステップ 8 [サーバとして帯域を制限する（Throttle as Server）] チェックボックスをオンにします。

ステップ 9 [認証済みとして扱う（Treat as Authenticated）] をオンにします。

ステップ 10 [OK] をクリックして、[承認済みホストの追加（Add Authorized Host）] ウィンドウを閉じます。

ステップ 11 IM and Presence サーバごとに手順 4 ～ 10 を繰り返します。

ステップ 12 すべてのホスト認証エントリを追加したら、[OK] を選択して、[フロントエンドサーバプロパティ（Front End Server Properties）] ウィンドウを閉じます。

次の作業

OCS フロントエンド サーバでのサービスの再起動, （4 ページ）

関連トピック

統合のトラブルシューティング

OCS フロントエンド サーバでのサービスの再起動

OCS ですべての設定手順が完了したら、OCS サービスを再起動し、設定を有効にする必要があります。

（注）
- この手順は、あらかじめスケジュールされたメンテナンスの時間帯に実施することをお勧めします。
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンド サーバでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 Standard Edition サーバまたは Enterprise Edition フロントエンド サーバの FQDN を右クリックし、[停止（Stop）] > [フロントエンド サービス（Front End Services）] > [フロントエンド サービス（Front End Service）] を選択します。

ステップ 3 サービスが停止したら、Standard Edition サーバまたは Enterprise Edition フロントエンド サーバの FQDN を右クリックし、[開始（Start）] > [フロントエンド サービス（Front End Services）] > [フロントエンド サービス（Front End Service）] を選択します。

関連トピック

統合のトラブルシューティング

TLS 暗号化の設定

IM and Presence および OCS 間の TLS 暗号化を設定するには、次の手順を実行する必要があります。

- 連邦情報処理標準コンプライアンスを OCS で有効にする, （6 ページ）
- TLS 相互認証の OCS での設定, （6 ページ）
- 認証局ルート証明書の OCS へのインストール, （7 ページ）
- 既存の OCS 署名付き証明書の検証, （10 ページ）
- 認証局からの署名付き証明書の要求, （11 ページ）

TLS の設定が完了したら、OCS サーバでサービスを再起動する必要があります。OCS フロントエンド サーバでのサービスの再起動, （4 ページ）を参照してください。

連邦情報処理標準コンプライアンスを OCS で有効にする

IM and Presence および OCS 間の TLS 暗号化をサポートするには、OCS サーバで TLSv1 を有効にする必要があります。 TLSv1 は連邦情報処理標準（FIPS）コンプライアンスの一環として Windows サーバに組み込まれています。 次の手順では、FIPS コンプライアンスを有効にする方法について説明しています。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンド サーバでこの手順を実行する必要があります。

手順

ステップ 1 OCS サーバで、[スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [ローカル セキュリティ ポリシー（Local Security Policy）] を選択します。

ステップ 2 コンソール ツリーから、[ローカル ポリシー（Local Policies）] を選択します。

ステップ 3 [セキュリティ オプション（Security Options）] を選択します。

ステップ 4 [システム暗号化：暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う（System Cryptography: Use FIPS Compliant algorithms for encryption, hashing and signing）] をダブルクリックします。

ステップ 5 セキュリティ設定を有効にします。

ステップ 6 [OK] を選択します。

ステップ 7 [ローカル セキュリティの設定（Local Security Setting）] ウィンドウを閉じます。

次の作業

TLS 相互認証の OCS での設定, （6 ページ）

関連トピック

統合のトラブルシューティング

TLS 相互認証の OCS での設定

IM and Presence および OCS 間の TLS 暗号化を設定するには、TLS 相互認証について OCS サーバでポート 5061 を設定する必要があります。 次の手順では、相互 TLS 認証用にポート 5061 を設定する方法について説明します。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンドサーバでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 Standard Edition サーバまたは Enterprise Edition フロントエンド サーバの FQDN を右クリックし、[プロパティ（Properties）] > [フロントエンドのプロパティ（Front End Properties）] を選択します。

ステップ 3 [全般（General）] タブを選択します。

ステップ 4 ポート 5061 に関連付けられた転送が **MTLS** の場合、手順 8 に進みます。

ステップ 5 ポート 5061 に関連付けられた転送が **MTLS** ではない場合、[編集（Edit）] を選択します。

ステップ 6 [転送（Transport）] ドロップダウン リストから **MTLS** を選択します。

ステップ 7 [OK] をクリックして、[接続の編集（Edit Connection）] ウィンドウを閉じます。 これで、ポート 5061 に関連付けられた転送は **MTLS** になるはずです。

ステップ 8 [OK] を選択して [プロパティ（Properties）] ウィンドウを閉じます。

次の作業

認証局ルート証明書の OCS へのインストール，（7 ページ）

関連トピック

統合のトラブルシューティング

認証局ルート証明書の OCS へのインストール

IM and Presence および OCS 間の TLS 暗号化をサポートするには、OCS サーバごとに署名付きセキュリティ証明書がなければなりません。 この署名付き証明書は、証明書に署名した認証局（CA）のルート証明書とともに、各 OCS サーバにインストールする必要があります。

OCS サーバと IM and Presence サーバで同じ CA を共有することをお勧めします。 共有していない場合、IM and Presence 証明書に署名した CA のルート証明書も各 OCS サーバにインストールする必要があります。

通常、OCS CA のルート証明書は各 OCS サーバにすでにインストールされています。 したがって、OCS と IM and Presence が同じ CA を共有している場合、ルート証明書のインストールは必要ない場合があります。 ただし、ルート証明書が必要な場合は、次の詳細を参照してください。

Microsoft 認証局を使用している場合、Microsoft 認証局から OCS へのルート証明書のインストールについて、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』に記載の次の手順を参照してください。

- CA 証明書チェーンのダウンロード
- CA 証明書チェーンのインストール

代替 CA を使用している場合、次の手順が、ルート証明書を OCS サーバにインストールする一般的な手順になります。 CA からルート証明書をダウンロードする手順は、選択した CA によって異なります。

はじめる前に

CA からルート証明書または証明書チェーンをダウンロードし、OCS サーバのハード ディスクに保存します。

手順

ステップ 1 OCS サーバで、[開始（Start）] > [実行（Run）] を選択します。

ステップ 2 **mmc** と入力し、[OK] を選択します。

ステップ 3 [ファイル（File）] メニューで、[スナップインの追加と削除（Add/Remove Snap-in）] を選択します。

ステップ 4 [スナップインの追加と削除（Add/Remove Snap-In）] ダイアログボックスで、[追加（Add）] を選択します。

ステップ 5 [利用できるスタンドアロン スナップイン（Available Standalone Snap-ins）] リストで、[証明書（Certificates）] を選択し、[追加（Add）] を選択します。

ステップ 6 [コンピュータ アカウント（Computer Account）] を選択し、[次へ（Next）] を選択します。

ステップ 7 [コンピュータの選択（Select Computer）] ダイアログ ボックスで、[<ローカル コンピュータ>（このコンソールを実行しているコンピュータ）（Local Computer (the computer this console is running on)）] チェックボックスをオンにし、[終了（Finish）] を選択します。

ステップ 8 [閉じる（Close）] を選択し、続いて [OK] を選択します。

ステップ 9 [証明書（Certificates）] コンソールの左側のペインで、[証明書（ローカル コンピュータ）（Certificates (Local Computer)）] を展開します。

ステップ 10 [信頼されたルート証明機関（Trusted Root Certification Authorities）] を展開します。

ステップ 11 [証明書（Certificates）] を右クリックし、[すべてのタスク（All Tasks）] を選択します。

ステップ 12 [インポート（Import）] を選択します。

ステップ 13 インポート ウィザードで [次へ（Next）] を選択します。

ステップ 14 [参照（Browse）]を選択して、ルート証明書または証明書チェーンを保存した場所に移動します。

ステップ 15 ファイルを選択し、[開く（Open）] を選択します。

ステップ 16 [次へ（Next）] を選択します。

ステップ 17 [証明書をすべて次のストアに配置する（Place all certificates in the following store）] というデフォルト値のままにして、[証明書ストア（Certificate store）] の下に [信頼されたルート証明機関（Trusted Root Certification Authorities）] が表示されていることを確認します。

ステップ 18 [次へ（Next）] を選択し、続いて [終了（Finish）] を選択します。

ステップ 19 他の CA について、必要に応じて手順 11 ～ 18 を繰り返します。

（注） 『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』マニュアルでは、Access Edge サーバについて説明しています。 パーティション イントラドメイン フェデレーションについては、Access Edge サーバへの参照を OCS Standard Edition サーバまたは Enterprise Edition フロントエンド サーバと置き換えることができます。

次の作業

既存の OCS 署名付き証明書の検証, （10 ページ）

関連トピック

統合のトラブルシューティング
『Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager』

既存の OCS 署名付き証明書の検証

IM and Presence および OCS 間の TLS 暗号化をサポートするには、OCS サーバごとに、クライアント認証をサポートする署名付きセキュリティ証明書がなければなりません。 署名付き証明書がすでに OCS サーバにインストールされている場合、次の手順では、その既存の署名付き証明書がクライアント認証をサポートしているかどうか確認する方法について説明します。

（注）

- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンド サーバでこの手順を実行する必要があります。

手順

ステップ 1 OCS サーバで、[開始（Start）] > [実行（Run）] を選択します。

ステップ 2 **mmc** と入力し、[OK] を選択します。

ステップ 3 [ファイル（File）] メニューで、[スナップインの追加と削除（Add/Remove Snap-in）] を選択します。

ステップ 4 [スナップインの追加と削除（Add/Remove Snap-In）] ダイアログボックスで、[追加（Add）] を選択します。

ステップ 5 [利用できるスタンドアロン スナップイン（Available Standalone Snap-ins）] リストで、[証明書（Certificates）] を選択し、[追加（Add）] を選択します。

ステップ 6 [コンピュータ アカウント（Computer Account）] を選択し、[次へ（Next）] を選択します。

ステップ 7 [コンピュータの選択（Select Computer）] ダイアログ ボックスで、[<ローカル コンピュータ>（このコンソールを実行しているコンピュータ）（Local Computer (the computer this console is running on)）] チェックボックスをオンにし、[終了（Finish）] を選択します。

ステップ 8 [閉じる（Close）] を選択し、続いて [OK] を選択します。

ステップ 9 [証明書（Certificates）] コンソールの左側のペインで、[証明書（ローカル コンピュータ）（Certificates (Local Computer)）] を展開します。

ステップ 10 [個人（Personal）] を展開して、[証明書（Certificates）] を選択します。

ステップ 11 右側のペインで、現在 OCS により使用されている署名付き証明書を見つけます。

ステップ 12 [クライアント認証（Client Authentication）] が [使用目的（Intended Purposes）] カラムに記載されていることを確認します。

次の作業

認証局からの署名付き証明書の要求, （11 ページ）

関連トピック

統合のトラブルシューティング

認証局からの署名付き証明書の要求

ここでは、次の手順について説明します。

- 署名付き証明書の OCS サーバへのインストール, （12 ページ）
- TLS ネゴシエーション用にインストールされた証明書の選択, （14 ページ）

（注） このトピックの手順は、OCS サーバに署名付き証明書が存在しない、または既存の証明書がクライアント認証をサポートしていない場合のみ必要です。

IM and Presence および OCS 間の TLS 暗号化をサポートするには、OCS サーバごとに、クライアント認証をサポートする署名付きセキュリティ証明書がなければなりません。 どの OCS サーバにも署名付きセキュリティ証明書がない場合、次の手順は、認証局から新たに署名した証明書を要求し、その特定の OCS サーバにインストールする方法の概要を説明します。

OCS からの証明書署名要求（CSR）で使用されている件名共通名（CN）は、OCS の展開により異なります。

- Standard Edition サーバの場合、Standard Edition サーバの FQDN を件名 CN として使用します。
- Enterprise Edition フロントエンド サーバの場合、フロントエンド サーバが属するプールの FQDN を件名 CN として使用します。

スタンドアロン Microsoft 認証局

スタンドアロン Microsoft 認証局を使用している場合、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』に記載の次の手順を参照して、OCS サーバの CA から署名付き証明書を要求します。

- CA サーバからの証明書の要求
- CA サーバからの証明書のダウンロード

（注） このマニュアルは Access Edge サーバについて説明しています。 パーティション イントラドメイン フェデレーションについては、Access Edge サーバへの参照を OCS Standard Edition サーバまたは Enterprise Edition フロントエンド サーバと置き換えることができます。

企業 Microsoft 認証局

企業 Microsoft 認証局を使用している場合、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』に記載の次の手順を参照して、CA で必要なテンプレートを生成し、OCS サーバの CA から署名付き証明書を要求します。

- 企業の認証局を使用した Access Edge のカスタム証明書の作成
- サイト サーバの署名付き証明書の要求

別の認証局

代替 CA を使用している場合、次の手順が、署名付き証明書を OCS サーバにインストールする一般的な手順になります。 署名付き証明書を要求する手順は、選択した CA によって異なります。

関連トピック

『Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager』

署名付き証明書の OCS サーバへのインストール

はじめる前に

CA から署名付き証明書をダウンロードし、OCS サーバのハード ディスクに保存します。

手順

ステップ 1 OCS サーバで、[開始（Start）] > [実行（Run）] を選択します。

ステップ 2 **mmc** と入力し、[OK] を選択します。

ステップ 3 [ファイル（File）] メニューで、[スナップインの追加と削除（Add/Remove Snap-in）] を選択します。

ステップ 4 [スナップインの追加と削除（Add/Remove Snap-In）] ダイアログボックスで、[追加（Add）] を選択します。

ステップ 5 [利用できるスタンドアロン スナップイン（Available Standalone Snap-ins）] リストで、[証明書（Certificates）] を選択し、[追加（Add）] を選択します。

ステップ 6 [コンピュータ アカウント（Computer Account）] を選択し、[次へ（Next）] を選択します。

ステップ 7 [コンピュータの選択（Select Computer）] ダイアログ ボックスで、[<ローカル コンピュータ>（このコンソールを実行しているコンピュータ）（Local Computer (the computer this console is running on)）] チェックボックスをオンにし、[終了（Finish）] を選択します。

ステップ 8 [閉じる（Close）] を選択し、続いて [OK] を選択します。

ステップ 9 [証明書（Certificates）] コンソールの左側のペインで、[証明書（ローカル コンピュータ）（Certificates (Local Computer)）] を展開します。

ステップ 10 [個人（Personal）] を展開します。

ステップ 11 [証明書（Certificates）] を右クリックし、[すべてのタスク（All Tasks）] を選択します。

ステップ 12 [インポート（Import）] を選択します。

ステップ 13 インポート ウィザードで [次へ（Next）] を選択します。

ステップ 14 [参照（Browse）] を選択して、署名付き証明書を保存した場所に移動します。

ステップ 15 ファイルを選択し、[開く（Open）] を選択します。

ステップ 16 [次へ（Next）] を選択します。

ステップ 17 [証明書をすべて次のストアに配置する（Place all certificates in the following store）] というデフォルト値のままにして、[証明書ストア（Certificate store）] の下に [個人（Personal）] が表示されていることを確認します。

ステップ 18 [次へ（Next）] を選択し、続いて [終了（Finish）] を選択します。

次の作業

TLS ネゴシエーション用にインストールされた証明書の選択, （14 ページ）

関連トピック

統合のトラブルシューティング

TLS ネゴシエーション用にインストールされた証明書の選択

使用されている CA に関係なく、署名付き証明書が OCS サーバにインストールされたら、次の手順を実行して、TLS が IM and Presence とネゴシエーションする場合に OCS が使用するインストール済み証明書を選択する必要があります。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 Standard Edition サーバまたは Enterprise Edition フロントエンド サーバの FQDN を右クリックし、[プロパティ（Properties）] > [フロントエンドのプロパティ（Front End Properties）] を選択します。

ステップ 3 [セキュリティ（Security）] タブを選択し、[証明書の選択（Select Certificate）] を選択します。

ステップ 4 インストール済み証明書のリストから、新たに署名された証明書を選択し、[OK] を選択して [証明書の選択（Select Certificate）] ウィンドウを閉じます。

ステップ 5 [OK] を選択して [プロパティ（Properties）] ウィンドウを閉じます。

次の作業

OCS フロントエンド サーバでのサービスの再起動, （4 ページ）

関連トピック

統合のトラブルシューティング