CHAPTER 40

外部メッセージ ストア内の電子メールへのアクセスの設定

外部メッセージ ストア内の電子メールへのユーザ アクセスについて

Cisco Unity Connection が外部メッセージ ストア（Cisco Unity Connection 以外のメッセージ ストア）に接続するよう設定されている場合、ユーザは、電話で Cisco Unity Connection にログインして、電子メールの再生を聞くことができます。この章では、ライセンスのあるユーザが電子メールを再生できるように Microsoft Exchange と Cisco Unity Connection を設定します。

次の各項を参照してください。

- Exchange 2007 メッセージ ストア内の電子メールへのアクセスの設定（P.40-2）
- Exchange 2003 メッセージ ストア内の電子メールへのアクセスの設定（P.40-8）

Exchange 2007 メッセージ ストア内の電子メールへのアクセスの設定

Exchange 2007 と連動するように Cisco Unity Connection を設定すると、ユーザは Exchange 2007 メッセージ ストア内の電子メールにアクセスできます。

次の各項を参照してください。

- Exchange 2007 電子メールへのユーザ アクセスを提供するためのタスク リスト（P.40-2）
- Exchange への IMAP アクセスの有効化（P.40-2）
- SSL による安全な IMAP の設定と SSL 証明書の有効化（Exchange 2007 のみ）（P.40-3）
- ユーザがアクセスできる Exchange サーバを指定するための Cisco Unity Connection 外部サービスの作成（P.40-5）
- 外部サービス用のユーザの設定（P.40-6）

Exchange 2007 電子メールへのユーザ アクセスを提供するためのタスク リスト

ユーザが Exchange 2007 メッセージ ストア内の電子メールにアクセスできるようにするには、次のタスクを記載どおりの順序で実行します。

1. Exchange への IMAP アクセスを有効にします。P.40-2 の「Exchange への IMAP アクセスの有効化」を参照してください。
2. アクセスする電子メール メッセージが配置された各 Exchange サーバ上で、SSL サーバ証明書を作成してインストールします。P.40-3 の「SSL による安全な IMAP の設定と SSL 証明書の有効化（Exchange 2007 のみ）」を参照してください。
3. Connection 外部サービスを作成します。P.40-5 の「ユーザがアクセスできる Exchange サーバを指定するための Cisco Unity Connection 外部サービスの作成」を参照してください。
4. 外部サービス用にユーザを設定します。P.40-6 の「外部サービス用のユーザの設定」を参照してください。
5. TTS 機能にアクセスするためのライセンスが提供されるサービス クラスにユーザを割り当てて、ユーザが TTS 機能を使用できるようにします。
6. ユーザごとに、ユーザのメールボックスが格納される Exchange サーバを指定するための外部サービスのアカウントを Connection で作成します。この作業によって、Connection に電話でログインしたユーザが電子メールにアクセスできるようになります。

Exchange への IMAP アクセスの有効化

Cisco Unity Connection は、IMAP プロトコルを使用して Exchange の電子メールにアクセスすることで、TTS を使用したメッセージの再生を実現しています。Exchange は、デフォルトではメッセージへの IMAP アクセスを許可するように設定されていません。ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持された各 Exchange サーバ上で、次の手順を実行して IMAP アクセスを有効にします。

Exchange への IMAP アクセスを有効にする

ステップ 1　ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持された Exchange サーバ上で、ローカル Administrators グループに所属す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］メニューで、［**管理ツール**］>［**サービス**］をクリックします。

ステップ 3　右ペインで、［**Microsoft Exchange IMAP4**］サービスを確認します。

ステップ 4　［状態］カラムの値が［**開始**］で、［スタートアップの種類］カラムの値が［**自動**］になっている場合は、ステップ 9 に進みます。

これ以外の値になっている場合は、［**Microsoft Exchange IMAP4**］をダブルクリックします。

ステップ 5　［Microsoft Exchange IMAP4 のプロパティ］ダイアログボックスで、［スタートアップの種類］が［自動］になっていない場合は［**自動**］に変更します。

ステップ 6　［サービスの状態］が［開始］になっていない場合は、［**開始**］をクリックします。

ステップ 7　［**OK**］をクリックして、［Microsoft Exchange IMAP4 のプロパティ］ダイアログボックスを閉じます。

ステップ 8　［サービス］MMC を閉じます。

ステップ 9　ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持された各 Exchange サーバ上で、ステップ 1 ～ステップ 8 を繰り返します。

SSL による安全な IMAP の設定と SSL 証明書の有効化（Exchange 2007 のみ）

SSL による安全な IMAP を設定し、SSL 証明書を有効にする（Exchange 2007 のみ）

ステップ 1　Exchange サーバで、**Exchange 管理シェル** アプリケーションを開きます。

ステップ 2　次のコマンドを入力します。<Exchange サーバ > は Exchange サーバの IP アドレスまたはホスト名で、< フレンドリ名 > は Exchange サーバに対して選択したフレンドリ名です。

new-exchangecertificate -generaterequest -domainname <Exchange サーバ > -friendlyname < フレンドリ名 >-path c:\csr.txt

注意　Exchange サーバのドメイン名は、IP アドレスまたは完全修飾 DNS 名（推奨）である必要があります。これにより、Connection サーバは Exchange サーバに対して正常に ping を実行できます。IP アドレスまたは完全修飾 DNS 名でない場合、ユーザが外部メッセージ ストア内の電子メールにアクセスできない可能性があります。

ステップ 3　**Enter** キーを押します。ルート ディレクトリに Csr.txt という名前の Certificate Signing Request（CSR; 証明書署名要求）ファイルが作成されます。

ステップ 4　この CSR ファイルを Certification Authority（CA; 認証局）に送信します。認証局によって新しい証明書が生成され、返送されます。

（注）　CA のパブリック ルート証明書またはパブリック ルート証明書チェーンのコピーを保持している必要があります。この証明書は、Exchange 2007 サーバを信頼するように Connection を設定するために必要です。

ステップ 5　次のコマンドを入力します。< パス > は、CA が新しいサーバ証明書を保存するディレクトリの場所です。

import-exchangecertificate -path < パス >

ステップ 6　**Enter** キーを押します。

ステップ 7　次のコマンドを入力します。

dir cert:\localmachine\my | fl

ステップ 8　**Enter** キーを押します。

ステップ 9　「フィンガープリント（thumbprint）」プロパティを強調表示し、**Ctrl-C** を押して、そのプロパティをクリップボードにコピーします。

ステップ 10　IMAP を使用して外部電子メール サーバからの電子メールにアクセスするように Connection を設定し、さらに Exchange 2007 からの予定表データを使用するようにも設定する場合は、次のコマンドを入力します。< フィンガープリント > は、ステップ 9 でコピーした「フィンガープリント（thumbprint）」です。

enable-exchangecertificate -thumbprint < フィンガープリント > -services "IIS,IMAP"

IMAP を使用するように Connection を設定せずに、Exchange 2007 からの予定表データを使用するように設定する場合は、次のコマンドを入力します。< フィンガープリント > は、ステップ 9 でコピーした「フィンガープリント（thumbprint）」です。

enable-exchangecertificate -thumbprint < フィンガープリント > -services "IIS"

ステップ 11　**Enter** キーを押します。

ステップ 12　データをクリア テキストとして送信する場合は、この手順の残りのステップをスキップし、P.40-5 の「ユーザがアクセスできる Exchange サーバを指定するための Cisco Unity Connection 外部サービスの作成」に進みます。クリア テキストとして送信しない場合は、**IIS マネージャ** アプリケーションを開きます。

ステップ 13　［**IIS**］>［< サーバ名 >］>［**Web サイト**］>［**既定の Web サイト**］に移動します。

ステップ 14　［**既定の Web サイト**］を右クリックし、［**プロパティ**］をクリックします。

ステップ 15　［プロパティ］ダイアログボックスで、［**ディレクトリ セキュリティ**］タブをクリックします。

ステップ 16　［セキュリティ保護された通信］で、［**編集**］をクリックします。

ステップ 17　［**セキュリティ保護されたチャネルを要求**］チェックボックスをオンにします。

ステップ 18　［**OK**］をクリックします。

ステップ 19　［プロパティ］ダイアログボックスで、［**OK**］をクリックします。

ユーザがアクセスできる Exchange サーバを指定するための Cisco Unity Connection 外部サービスの作成

Cisco Unity Connection の管理で、ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持された Exchange サーバごとに、それぞれ 1 つの IMAP サービスを作成し、設定します。

Cisco Unity Connection ユーザが電子メールにアクセスできる Exchange サーバを指定する

ステップ 1　Cisco Unity Connection の管理で、［**システム設定（System Settings）**］を展開し、［**外部サービス（External Services）**］をクリックします。

ステップ 2　［外部サービスの検索（Search External Services）］ページで、［**新規追加（Add New）**］をクリックします。

ステップ 3　［外部サービスの新規作成（New External Service）］ページの［タイプ（Type）］リストで、［**Exchange 2007 External Service Template**］をクリックします。

ステップ 4　［**有効にする（Enabled）**］チェックボックスがオンになっていることを確認します。

ステップ 5　各自の電子メールにアクセスできるように Connection ユーザを設定するときにサービスの識別に役立つ名前を、［表示名（Display Name）］フィールドに入力します（たとえば、サービスの名前の中に、ユーザのアクセスする電子メールが保持された Exchange サーバの名前を含めます）。

ステップ 6　［サーバ（Server）］フィールドに、ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持されたいずれかの Exchange サーバのサーバ名または完全修飾ドメイン名を入力します。

入力する値は、Exchange サーバの証明書に含まれているサーバ名または完全修飾ドメイン名と一致する必要があります。

ステップ 7　［認証モード（Authentication Mode）］リストで、［**NTLM**］をクリックします。

ステップ 8　SSL 証明書を作成してインストールした場合は、［セキュリティトランスポートのタイプ（Security Transport Type）］リストの［**SSL**］をクリックします。それ以外の場合は［**なし（None）**］をクリックします。

ステップ 9　ステップ 8 で［SSL］を選択した場合は、［**サーバ証明書を確認にする（Validate Server Certificate）**］チェックボックスをオンにします。それ以外の場合は、ステップ 10 に進みます。

ステップ 10　［サービス機能（Service Capabilities）］で、［**サードパーティのメッセージ ストア内の電子メールへのユーザ アクセス（User Access to Email in Third-Party Message Store）**］チェックボックスをオンにします。

ステップ 11　［**保存（Save）**］をクリックします。

ステップ 12　ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持されたこの他の Exchange 2007 サーバごとに、ステップ 2 ～ステップ 13 を繰り返します。

ステップ 13　Cisco Unity Connection の管理を閉じます。

外部サービス用のユーザの設定

次の手順を実行します。

（注）　Exchange は、設定する Connection ユーザごとにユーザを必要とします。

外部サービス用にユーザを設定する

ステップ 1　Cisco Unity Connection の管理で、[**(ユーザ (Users)**] を展開し、[**ユーザ (Users)**] をクリックします。

ステップ 2　[ユーザの検索（Search Users）] ページで、ユーザのエイリアスをクリックします。

ステップ 3　[ユーザの基本設定の編集（Edit User Basics）] ページで、[編集（Edit）] メニューの [**外部サービスのアカウント（External Service Accounts）**] をクリックします。

ステップ 4　[外部サービスのアカウント（External Service Accounts）] ページで、[**新規追加（Add New）**] をクリックします。

ステップ 5　[外部サービスのアカウントの新規作成（New External Service Accounts）] ページの [外部サービス（External Service）] フィールドで、P.40-5 の「ユーザがアクセスできる Exchange サーバを指定するための Cisco Unity Connection 外部サービスの作成」で作成した適切な外部サービスの表示名をクリックします。

ステップ 6　[電子メール（Email Address）] フィールドに、ユーザの電子メール アドレスを入力します。

ステップ 7　[ログイン タイプ（Login Type）] フィールドで、次の適切なオプションをクリックします。

- [**接続エイリアスを使用（Use Connection Alias）**]：このオプションは、Exchange 2007 の [ユーザー ID] 設定が Connection ユーザ エイリアスと同一である場合に便利です。Connection は、Connection ユーザ エイリアスを使用してユーザをログインさせます。
- [**次のユーザ ID を使用：（Use User ID Provided Below）**]：Exchange 2007 の [ユーザー ID] 設定を入力します（[ユーザー ID] 設定が Connection ユーザ エイリアスと異なる場合に便利です）。Connection は、このフィールドの設定を使用してユーザをログインさせます。

ステップ 8　*（ステップ 7 で [次のユーザ ID を使用：（Use User ID Provided Below）] オプションを選択した場合のみ）*[ユーザ ID（User ID）] フィールドに、Exchange の [ユーザー ID] 設定を入力します。

ステップ 9　[パスワード（Password）] フィールドに、Exchange のパスワードを入力します。Connection は、このフィールドの設定を使用してユーザをログインさせます。

ステップ 10　[サービス機能（Service Capabilities）] で、[**サードパーティのメッセージ ストア内の電子メールへのユーザ アクセス（User Access to Email in Third-Party Message Store）**] チェックボックスをオンにします。

ステップ 11　[**保存（Save）**] をクリックします。

ステップ 12　ユーザの Exchange 設定を確認するには、[**テスト（Test）**] をクリックします。[タスクの実行結果（Task Execution Results）] ウィンドウにテスト結果が表示されます。

テストのいずれかの部分が失敗した場合は、Exchange、Cisco Unity Connection、およびユーザの設定を確認します。

ステップ 13 残りすべてのユーザについて、ステップ 2 ～ステップ 12 を繰り返します。

Exchange 2003 メッセージ ストア内の電子メールへのアクセスの設定

Exchange 2003 と連動するように Cisco Unity Connection を設定すると、ユーザは Exchange 2003 メッセージ ストア内の電子メールにアクセスできます。

次の各項を参照してください。

- Exchange 2003 電子メールへのユーザ アクセスを提供するためのタスク リスト（P.40-8）
- Exchange への IMAP アクセスの有効化（P.40-9）
- Active Directory サービス アカウントの作成と設定（Exchange 2003 のみ）（P.40-9）
- SSL 証明書の作成とインストール（Exchange 2003 のみ）（P.40-11）
- Cisco Unity Connection と Exchange 間での安全な通信の要求（Exchange 2003 のみ）（P.40-16）
- Exchange 証明書を信頼するための Cisco Unity Connection サーバの設定（Exchange 2003 のみ）（P.40-17）
- ユーザがアクセスできる Exchange サーバを指定するための Cisco Unity Connection 外部サービスの作成（P.40-19）
- 外部サービス用のユーザの設定（P.40-20）

Exchange 2003 電子メールへのユーザ アクセスを提供するためのタスク リスト

ユーザが Exchange 2003 メッセージ ストア内の電子メールにアクセスできるようにするには、次のタスクを記載どおりの順序で実行します。

1. Exchange 2003 への IMAP アクセスを有効にします。P.40-9 の「Exchange への IMAP アクセスの有効化」を参照してください。
2. Connection が Exchange データへのアクセスに使用する Active Directory サービス アカウントを作成し、必要な権限を付与します。P.40-9 の「Active Directory サービス アカウントの作成と設定（Exchange 2003 のみ）」を参照してください。
3. アクセスする電子メール メッセージが配置された各 Exchange サーバ上で、SSL サーバ証明書を作成してインストールします。P.40-11 の「SSL 証明書の作成とインストール（Exchange 2003 のみ）」を参照してください。
4. *（省略可能、ただし推奨）* Web クライアント（Connection を含む）からの暗号化されていない通信を拒否するように IIS を設定します。P.40-16 の「Cisco Unity Connection と Exchange 間での安全な通信の要求（Exchange 2003 のみ）」を参照してください。
5. Exchange サーバ上に作成してインストールした SSL 証明書を信頼するように Connection を設定します。P.40-17 の「Exchange 証明書を信頼するための Cisco Unity Connection サーバの設定（Exchange 2003 のみ）」を参照してください。
6. Connection 外部サービスを作成します。P.40-19 の「ユーザがアクセスできる Exchange サーバを指定するための Cisco Unity Connection 外部サービスの作成」を参照してください。
7. 外部サービス用にユーザを設定します。P.40-20 の「外部サービス用のユーザの設定」を参照してください。
8. TTS 機能にアクセスするためのライセンスが提供されるサービス クラスにユーザを割り当てて、ユーザが TTS 機能を使用できるようにします。
9. ユーザごとに、ユーザのメールボックスが格納される Exchange サーバを指定するための外部サービスのアカウントを Connection で作成します。この作業によって、Connection に電話でログインしたユーザが電子メールにアクセスできるようになります。

Exchange への IMAP アクセスの有効化

Cisco Unity Connection は、IMAP プロトコルを使用して Exchange の電子メールにアクセスすることで、TTS を使用したメッセージの再生を実現しています。Exchange は、デフォルトではメッセージへの IMAP アクセスを許可するように設定されていません。ライセンスのある Connection ユーザが TTS を使用して再生する電子メールが保持された各 Exchange サーバ上で、次の手順を実行して IMAP アクセスを有効にします。

Exchange への IMAP アクセスを有効にする

ステップ 1　ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持された Exchange サーバ上で、ローカル Administrators グループに所属す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］メニューで、［管理ツール］>［サービス］をクリックします。

ステップ 3　右ペインで、［**Microsoft Exchange IMAP4**］サービスを確認します。

ステップ 4　［状態］カラムの値が［開始］で、［スタートアップの種類］カラムの値が［自動］になっている場合は、ステップ 9 に進みます。

これ以外の値になっている場合は、［**Microsoft Exchange IMAP4**］をダブルクリックします。

ステップ 5　［Microsoft Exchange IMAP4 のプロパティ］ダイアログボックスで、［スタートアップの種類］が［自動］になっていない場合は［自動］に変更します。

ステップ 6　［サービスの状態］が［開始］になっていない場合は、［開始］をクリックします。

ステップ 7　［**OK**］をクリックして、［Microsoft Exchange IMAP4 のプロパティ］ダイアログボックスを閉じます。

ステップ 8　［サービス］MMC を閉じます。

ステップ 9　ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持された各 Exchange サーバ上で、ステップ 1 ～ステップ 8 を繰り返します。

Active Directory サービス アカウントの作成と設定（Exchange 2003 のみ）

Cisco Unity Connection は、Connection のプロキシとして機能する Active Directory アカウントを使用して Exchange 2003 電子メールにアクセスします。次の手順を実行してサービス アカウントを作成し、必要な権限を付与してください。

Exchange 電子メールにアクセスできるサービス アカウントを作成して設定する

ステップ 1　［Active Directory ユーザーとコンピュータ］と Exchange システム マネージャがインストールされたコンピュータ上で、Domain Administrators グループに所属す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］メニューで、［プログラム］>［**Microsoft Exchange**］>［**Active Directory ユーザーとコンピュータ**］をクリックします。

ステップ 3　左ペインで、[< サーバ名 >] を展開し、[**Users**] を右クリックして、[新規作成] > [ユーザー] をクリックします。

ステップ 4　画面の指示に従って、ドメイン ユーザ アカウントを作成します。メールボックスは作成しないでください。

ステップ 5　Windows の [スタート] メニューで、[プログラム] > [**Microsoft Exchange**] > [システム マネージャ] をクリックします。

ステップ 6　左ペインで、[サーバー] を展開します。

ステップ 7　Cisco Unity Connection がアクセスするメールボックスを保持している Exchange サーバの名前を右クリックし、[プロパティ] をクリックします。

ステップ 8　[< サーバ名 > のプロパティ] ダイアログボックスで、[セキュリティ] タブをクリックします。

ステップ 9　[追加] をクリックします。

ステップ 10　[ユーザー、コンピュータ、またはグループの選択] ダイアログボックスの [選択するオブジェクト名を入力してください] フィールドに、ステップ 4 で作成したサービス アカウントの名前を入力します。

ステップ 11　[名前の確認] をクリックします。

ステップ 12　[**OK**] をクリックしてダイアログボックスを閉じます。

ステップ 13　[< サーバ名 > のプロパティ] ダイアログボックスの [グループ名またはユーザー名] リストで、サービス アカウントの名前をクリックします。

ステップ 14　[< アカウント名 > のアクセス許可] リストで権限を設定します。

a.　[フル コントロール] の [拒否] チェックボックスをオンにします。

b.　[Receive As] の [許可] チェックボックスをオンにします。

ステップ 15　[**OK**] をクリックして [< サーバ名 > のプロパティ] ダイアログボックスを閉じます。

ステップ 16　アクセスする電子メールが保持されたこの他の Exchange サーバごとに、ステップ 7 ～ステップ 15 を繰り返します。

SSL 証明書の作成とインストール（Exchange 2003 のみ）

この項では、ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持された各 Exchange サーバ上で、SSL 証明書を作成し、インストールします。証明書を導入すると、P.40-9 の「Active Directory サービス アカウントの作成と設定（Exchange 2003 のみ）」で作成したサービス アカウントの資格情報を、暗号化されていない状態で Cisco Unity Connection がネットワーク経由で送信することがなくなります。また、Exchange が電子メールの内容を暗号化されていない状態でネットワーク経由で送信することもなくなります。

この他の方法で証明書を作成およびインストールする場合は、適切なドキュメントを参照してください。

この項では、4 つの手順について説明します。これらの手順を実行する場合は、記述されている順序どおりに実行してください。

次の方法で SSL 証明書を発行する場合は、それぞれの手順に従ってください。

- Microsoft 証明書サービス : ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持された Exchange サーバと同じドメインにある任意のサーバで、以降の手順を実行します。
- この他のアプリケーション：インストール手順については、それぞれのアプリケーションのドキュメントを参照してください。次に、P.40-12 の手順「証明書署名要求を作成する」に進みます。
- 外部の認証局：P.40-12 の手順「証明書署名要求を作成する」に進みます。

Microsoft 証明書サービス コンポーネントをインストールする

ステップ 1　Windows Server 2003 のディスクを用意します。Microsoft 証明書サービス コンポーネントをインストールする過程で、このディスクを使用するように要求される場合があります。

ステップ 2　ローカル Administrators グループに所属するアカウントを使用して、Windows にログインします。

ステップ 3　Windows の［スタート］メニューから［**設定**］>［**コントロール パネル**］>［**プログラムの追加と削除**］をクリックします。

ステップ 4　［プログラムの追加と削除］コントロール パネルの左ペインで、［**Windows コンポーネントの追加と削除**］をクリックします。

ステップ 5　［Windows コンポーネント］ダイアログボックスで、［**証明書サービス**］チェックボックスをオンにします。この他の項目は変更しないでください。

ステップ 6　コンピュータ名およびドメイン　メンバシップの変更ができなくなるという警告が表示された場合は、［**はい**］をクリックします。

ステップ 7　［**次へ**］をクリックします。

ステップ 8　［証明機関の種類］ページで、［**スタンドアロンのルート CA**］をクリックし、［**次へ**］をクリックします（スタンドアロンの認証局（CA）は、Active Directory を必要としない CA です）。

ステップ 9　［CA 識別情報］ページの［この CA の共通名］フィールドに、認証局の名前を入力します。

ステップ 10　［識別名のサフィックス］フィールドで、デフォルト値をそのまま使用します。

ステップ 11　［有効期間］で、デフォルト値の［**5 年**］をそのまま使用します。

ステップ 12［次へ］をクリックします。

ステップ 13［証明書データベースの設定］ページで、［次へ］をクリックしてデフォルト値をそのまま使用します。

コンピュータ上でインターネット インフォメーション サービスが動作しているため、停止してから処理を続行する必要があるというメッセージが表示された場合は、［はい］をクリックしてサービスを停止します。

ステップ 14 Windows Server 2003 ディスクをドライブに挿入するように要求された場合は、Cisco Unity Connection ディスク（同じ必須ソフトウェアが収録されています）または Windows Server 2003 ディスクを挿入します。

ステップ 15［Windows コンポーネント ウィザードの完了］ダイアログボックスで、［完了］をクリックします。

ステップ 16［プログラムの追加と削除］ダイアログボックスを閉じます。

ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持された Exchange サーバごとに、次の手順を実行します。

証明書署名要求を作成する

ステップ 1 Exchange システム マネージャがインストールされたサーバ上で、［Exchange 管理者 (完全)］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］メニューで、［プログラム］>［**Microsoft Exchange**］>［システム マネージャ］をクリックします。

ステップ 3 左ペインで、［< 組織 >］>［管理グループ］>［< 管理グループ >］>［サーバー］>［< サーバ名 >］>［プロトコル］>［**IMAP4**］を展開します。< 管理グループ > および < サーバ名 > は、ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持された最初の Exchange サーバです。

ステップ 4［既定の **IMAP4** 仮想サーバー］を右クリックし、［プロパティ］をクリックします。

ステップ 5［既定の IMAP4 仮想サーバーのプロパティ］ダイアログボックスで、［アクセス］タブをクリックします。

ステップ 6［証明書］をクリックします。

ステップ 7［Web サーバー証明書ウィザードの開始］ページで、［次へ］をクリックします。

ステップ 8［サーバー証明書］ページで、［証明書の新規作成］をクリックします。

ステップ 9［次へ］をクリックします。

ステップ 10［証明書の要求の送信方法］ページで、［証明書の要求を作成して後で送信する］をクリックします。

ステップ 11［次へ］をクリックします。

ステップ 12［名前とセキュリティの設定］ページで、証明書の名前（< サーバ名 >_Cert など）を入力します。

ステップ 13［次へ］をクリックします。

ステップ 14［組織に関する情報］ページで、適切な値を入力します。

ステップ 15［次へ］をクリックします。

ステップ 16［サイトの一般名］ページで、Exchange サーバのコンピュータ名または完全修飾ドメイン名を入力します。

コンピュータ名と完全修飾ドメイン名のどちらを指定したかを覚えておいてください。この情報は以降の手順で必要になります。

注意　この名前は、安全な接続を使用してシステムにアクセスするための URL に含まれている、ホスト名の部分と完全に一致する必要があります。

ステップ 17［次へ］をクリックします。

ステップ 18［地理情報］ページで、適切な情報を入力します。

ステップ 19［次へ］をクリックします。

ステップ 20［証明書要求ファイル名］ページで、パスとファイル名を入力し、この情報を書き留めます。この情報は以降の手順で必要になります。

このサーバが P.40-11 の手順「Microsoft 証明書サービス コンポーネントをインストールする」で Microsoft 証明書サービスをインストールしたサーバではない場合は、現在のサーバから、および Microsoft 証明書サービスがインストールされたサーバからアクセスできるネットワーク ロケーションを選択するようにしてください。

ステップ 21［次へ］をクリックします。

ステップ 22［要求ファイルの概要］ページで、［次へ］をクリックします。

ステップ 23［Web サーバー証明書ウィザードの完了］ページで、［完了］をクリックします。

ステップ 24［**OK**］をクリックして、［既定の IMAP4 仮想サーバーのプロパティ］ダイアログボックスを閉じます。

ステップ 25 ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持されたこの他の Exchange サーバごとに、ステップ 3 ～ステップ 24 を繰り返して証明書署名要求を作成します。

ステップ 26 Exchange システム マネージャを閉じます。

ステップ 27 Microsoft 証明書サービスが別のサーバ上にあり、そのサーバからアクセスできるネットワーク ロケーションに証明書要求ファイルを保存できなかった場合は、証明書要求ファイルをリムーバブル メディア（フロッピーディスク、CD、または DVD）にコピーします。

ステップ 28 外部の認証局を使用しない場合、手順はこれで完了です。

外部の認証局を使用する場合は、ステップ 20 で指定した証明書要求ファイルを CA に送信します。CA から証明書が返された後、P.40-15 の手順「サーバ証明書をインストールする」に進みます。

P.40-12 の手順「証明書署名要求を作成する」で作成した証明書署名要求ごとに、証明書を発行するか、または発行してもらいます。

- Microsoft 証明書サービスを使用して証明書を発行する場合は、以降の手順を実行します。
- Microsoft 証明書サービス以外のアプリケーションを使用する場合は、そのアプリケーションのマニュアルを参照して、サーバ証明書を発行し、信頼する証明書をエクスポートしてください。信頼する証明書をエクスポートするときは、.pem ファイル名拡張子の付いた Base-64 符号化 X.509 形式でエクスポートします。この証明書は、この章の以降の手順で Cisco Unity Connection サーバにアップロードします。エクスポートした後、P.40-15 の手順「サーバ証明書をインストールする」に進みます。
- 証明書の発行に外部の認証局（CA）を使用する場合は、証明書署名要求を CA に送信します。CA に対して、.pem ファイル名拡張子の付いた Base-64 符号化 X.509 形式の信頼する証明書を要求します。この証明書は、この章の以降の手順で Cisco Unity Connection サーバにアップロードします。証明書が返された後、P.40-15 の手順「サーバ証明書をインストールする」に進みます。

サーバ証明書を発行する（Microsoft 証明書サービスを使用して証明書を発行する場合のみ）

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上で、Domain Admins グループに所属す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］メニューで、［**プログラム**］>［**管理ツール**］>［**証明機関**］をクリックします。

ステップ 3 左ペインで、［**証明機関（ローカル）**］>［**< 認証局名 >**］を展開します。< 認証局名 > は、P.40-11 の手順「Microsoft 証明書サービス コンポーネントをインストールする」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です。

ステップ 4 認証局の名前を右クリックし、［**すべてのタスク**］>［**新しい要求の送信**］をクリックします。

ステップ 5 ［要求ファイルを開く］ダイアログボックスで、P.40-12 の手順「証明書署名要求を作成する」で作成した最初の証明書署名要求ファイルの場所を参照し、ファイルをダブルクリックします。

ステップ 6 ［証明機関］の左ペインで、［**保留中の要求**］をクリックします。

ステップ 7 ステップ 5 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**］>［**発行**］をクリックします。

ステップ 8 ［証明機関］の左ペインで、［**発行した証明書**］をクリックします。

ステップ 9 新しい証明書を右クリックし、［**すべてのタスク**］>［**バイナリ データのエクスポート**］をクリックします。

ステップ 10 ［バイナリ データのエクスポート］ダイアログボックスで、［バイナリ データを含む列］リストの［**バイナリ証明書**］をクリックします。

ステップ 11 ［**バイナリ データをファイルに保存する**］をクリックします。

ステップ 12 ［**OK**］をクリックします。

ステップ 13 ［バイナリ データの保存］ダイアログボックスで、パスとファイル名を入力し、この情報を書き留めます。この情報は以降の手順で必要になります。

このサーバに Exchange システム マネージャがインストールされていない場合は、現在のサーバから、および Microsoft 証明書サービスがインストールされたサーバからアクセスできるネットワーク ロケーションを選択するようにしてください。

ステップ 14 ［**OK**］をクリックします。

ステップ 15 P.40-12 の手順「証明書署名要求を作成する」で証明書署名要求を複数作成した場合は、［発行した証明書］に表示されている証明書署名要求ごとに、ステップ 9 ～ステップ 11 を繰り返します。

ステップ 16 ［証明機関］を閉じます。

ステップ 17 Exchange システム マネージャが別のサーバ上にあり、そのサーバからアクセスできるネットワーク ロケーションに証明書要求ファイルを保存できなかった場合は、証明書要求ファイルをリムーバブル メディア（フロッピーディスク、CD、または DVD）にコピーします。

ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持された Exchange サーバごとに、次の手順を実行します。

サーバ証明書をインストールする

ステップ 1 Exchange システム マネージャがインストールされたコンピュータ上で、［Exchange 管理者 (完全)］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］メニューで、［**プログラム**］>［**Microsoft Exchange**］>［**システム マネージャ**］をクリックします。

ステップ 3 左ペインで、［< **組織名** >］>［**管理グループ**］>［< **管理グループ** >］>［**サーバー**］>［< **サーバ名** >］>［**プロトコル**］>［**IMAP4**］を展開します。< 管理グループ > および < サーバ名 > は、ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持された最初の Exchange サーバです。

ステップ 4 ［**既定の IMAP4 仮想サーバー**］を右クリックし、［**プロパティ**］をクリックします。

ステップ 5 ［**アクセス**］タブをクリックします。

ステップ 6 ［**証明書**］をクリックします。

ステップ 7 ［Web サーバー証明書ウィザードの開始］で、［**次へ**］をクリックします。

ステップ 8 ［保留中の証明書の要求］ページで、［**保留中の要求を処理し、証明書をインストールする**］をクリックします。

ステップ 9 ［**次へ**］をクリックします。

ステップ 10 ［保留中の要求を処理］ページで、証明書を保存した場所を参照し、Microsoft 証明書サービスまたはその他のアプリケーションを使用して作成したサーバ証明書、あるいは外部の CA から取得したサーバ証明書を指定します。

必要に応じて、［ファイルの種類］リストの値を［すべてのファイル (*.*)］に変更して証明書を表示します。

ステップ 11 ［次へ］をクリックします。

ステップ 12 ［証明書の概要］ページで、［次へ］をクリックします。

ステップ 13 ［Web サーバー証明書ウィザードの完了］ページで、［完了］をクリックします。

ステップ 14 ［既定の IMAP4 仮想サーバーのプロパティ］ダイアログボックスを閉じます。

ステップ 15 インストールする証明書ごとに、ステップ 3 ～ステップ 14 を繰り返します。

ステップ 16 Exchange システム マネージャを閉じます。

Cisco Unity Connection と Exchange 間での安全な通信の要求（Exchange 2003 のみ）

ここまでの手順で、Exchange への IMAP アクセスを有効にし、Cisco Unity Connection サーバと 1 つまたはそれ以上の Exchange サーバ間の IMAP 接続をセキュリティで保護しました。安全でない IMAP 接続を使用したアクセスが Exchange で許可されないようにするには、Cisco Unity Connection がアクセスできるようにする各 Exchange サーバ上で、次の手順を実行します。

Cisco Unity Connection との安全な通信を要求するように Exchange を設定する（省略可能、ただし推奨）

ステップ 1 ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持された Exchange サーバ上で、［Exchange 管理者 (完全)］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］メニューで、［プログラム］>［**Microsoft Exchange**］>［システム マネージャ］をクリックします。

ステップ 3 左ペインで、［サーバー］>［< サーバ名 >］>［プロトコル］>［**IMAP4**］>［既定の **IMAP4** 仮想サーバー］を展開します。

ステップ 4 ［既定の **IMAP4** 仮想サーバー］を右クリックし、［プロパティ］をクリックします。

ステップ 5 ［アクセス］タブをクリックします。

ステップ 6 ［通信］をクリックします。

ステップ 7 ［セキュリティ保護されたチャネルを要求］をクリックします。

ステップ 8 ［**OK**］をクリックします。

ステップ 9 ［プロパティ］ダイアログボックスを閉じます。

ステップ 10 左ペインで、同じサーバの［**サーバー**］>［**< サーバ名 >**］>［**プロトコル**］>［**IMAP4**］>［**既定の IMAP4 仮想サーバー**］を展開します。

ステップ 11 システム マネージャのツールバーにある［**停止**］アイコンをクリックします。

ステップ 12 数秒間、待機します。

ステップ 13［**再生**］アイコンをクリックします。

ステップ 14 ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持されたこの他の Exchange サーバごとに、ステップ 1 ～ステップ 13 を繰り返します。

Exchange 証明書を信頼するための Cisco Unity Connection サーバの設定（Exchange 2003 のみ）

Exchange サーバの証明書を Cisco Unity Connection サーバで信頼するには、Connection サーバ上のルート証明書ストアに、証明書を発行した各認証局の信頼できる証明書をアップロードする必要があります。通常は、すべての証明書を同じ認証局（たとえば、Microsoft 証明書サービスや VeriSign）を使用して発行します。

Exchange 証明書を信頼するように Cisco Unity Connection サーバを設定する

ステップ 1 Microsoft 証明書サービスを使用して証明書を発行した場合は、ステップ 2 に進みます。

この他のアプリケーションまたは外部の認証局を使用して証明書を発行した場合は、ステップ 21 に進み、信頼する証明書を Connection サーバ上のルート証明書ストアに Base-64 符号化 X.509 形式でアップロードします。

ステップ 2 Microsoft 証明書サービスをインストールしたサーバ上で、ローカル Administrators グループに所属するアカウントを使用して Windows にログインします。

ステップ 3 Windows の［スタート］メニューで、［**プログラム**］>［**管理ツール**］>［**証明機関**］をクリックします。

ステップ 4 左ペインで、［**証明機関 (ローカル)**］を展開します。

ステップ 5 認証局の名前を右クリックし、［**プロパティ**］をクリックします。

ステップ 6［< 認証局名 > のプロパティ］ダイアログボックスの［**全般**］タブにある［CA 証明書］リストで、Exchange サーバに対して発行したいずれかの証明書の名前をクリックします。

ステップ 7［**証明書の表示**］をクリックします。

ステップ 8［証明書］ダイアログボックスで、［**詳細設定**］タブをクリックします。

ステップ 9［**ファイルにコピー**］をクリックします。

ステップ 10［証明書のエクスポート ウィザードの開始］ページで、［**次へ**］をクリックします。

ステップ 11［エクスポート ファイルの形式］ページで、［**Base 64 encoded X.509 (.CER)**］をクリックします。

ステップ 12［次へ］をクリックします。

ステップ 13［エクスポートするファイル］ページで、信頼する証明書の一時的なパスおよびファイル名（c:\cacert.pem など）を入力します。ファイル名の拡張子は **.pem** を使用します。

注意　信頼する証明書は、ファイル名の拡張子を .pem にする必要があります。これ以外の場合、Connection サーバにアップロードできません。

ステップ 14 パスとファイル名を書き留めます。この情報は以降の手順で必要になります。

ステップ 15［次へ］をクリックします。

ステップ 16［証明書のエクスポート ウィザードの完了］ページで、［完了］をクリックします。

ステップ 17［**OK**］をクリックして［正しくエクスポートされました。］メッセージ ボックスを閉じます。

ステップ 18［**OK**］をクリックして［証明書］ダイアログボックスを閉じます。

ステップ 19［**OK**］をクリックして［< サーバ名 > のプロパティ］ダイアログボックスを閉じます。

ステップ 20［証明機関］を閉じます。

ステップ 21 信頼する証明書を Connection サーバがアクセスできるネットワーク ロケーションにコピーします。

ステップ 22 Connection サーバ上で、Cisco Unified オペレーティングシステムの管理にログインします。

ステップ 23［セキュリティ（Security）］メニューで、［証明書の管理（**Certificate Management**）］をクリックします。

ステップ 24［証明書の一覧（Certificate List）］ページで、［証明書のアップロード（**Upload Certificate**）］をクリックします。

ステップ 25［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、［**Connection-trust**］をクリックします。

ステップ 26［ルート証明書（Root Certificate）］フィールドで、Microsoft 証明書サービスまたはその他の認証局を使用して発行した証明書ファイル、あるいは CA から取得した証明書ファイルの名前を入力します。

ステップ 27［参照（**Browse**）］をクリックします。

ステップ 28［ファイルの選択］ダイアログボックスで、証明書ファイルの場所を参照し、ファイル名をクリックして、［開く］をクリックします。

ステップ 29［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**）］をクリックします。

ステップ 30［ステータス（Status）］領域で、アップロードが成功したと報告された後、［閉じる（**Close**）］をクリックします。

ステップ 31 複数の証明書を発行した場合、または複数の認証局から証明書が発行された場合は、信頼する証明書ごとにステップ 24 ～ステップ 30 を繰り返します。

ユーザがアクセスできる Exchange サーバを指定するための Cisco Unity Connection 外部サービスの作成

Cisco Unity Connection の管理で、ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持された Exchange サーバごとに、それぞれ 1 つの IMAP サービスを作成し、設定します。

Cisco Unity Connection ユーザが電子メールにアクセスできる Exchange サーバを指定する

ステップ 1 Cisco Unity Connection の管理で、［**システム設定（System Settings）**］を展開し、［**外部サービス（External Services）**］をクリックします。

ステップ 2 ［外部サービスの検索（Search External Services）］ページで、［**新規追加（Add New）**］をクリックします。

ステップ 3 ［外部サービスの新規作成（New External Service）］ページの［タイプ（Type）］リストで、［**Exchange 2003 External Service Template**］をクリックします。

ステップ 4 ［**有効にする（Enabled）**］チェックボックスがオンになっていることを確認します。

ステップ 5 各自の電子メールにアクセスできるように Connection ユーザを設定するときにサービスの識別に役立つ名前を、［表示名（Display Name）］フィールドに入力します（たとえば、サービスの名前の中に、ユーザのアクセスする電子メールが保持された Exchange サーバの名前を含めます）。

ステップ 6 ［サーバ（Server）］フィールドに、ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持されたいずれかの Exchange サーバのサーバ名または完全修飾ドメイン名を入力します。

入力する値は、P.40-12 の手順「証明書署名要求を作成する」のステップ 16 で指定した、Exchange サーバの証明書に含まれているサーバ名または完全修飾ドメイン名と一致する必要があります。

ステップ 7 ［認証モード（Authentication Mode）］リストで、［**NTLM**］をクリックします。

ステップ 8 SSL 証明書を作成してインストールした場合は、［セキュリティトランスポートのタイプ（Security Transport Type）］リストの［**SSL**］をクリックします。それ以外の場合は［**なし（None）**］をクリックします。

ステップ 9 ステップ 8 で［SSL］を選択した場合は、［**サーバ証明書を確認にする（Validate Server Certificate）**］チェックボックスをオンにします。それ以外の場合は、ステップ 10 に進みます。

ステップ 10 ［サービス クレデンシャル（Service Credentials）］フィールドに、P.40-9 の手順「Exchange 電子メールにアクセスできるサービス アカウントを作成して設定する」で作成したサービス アカウントの Active Directory ユーザ ログイン名を入力します。**< ドメイン名 >\< アカウント名 >** 形式を使用してください。

ステップ 11 ［パスワード（Password）］フィールドに、サービス アカウントのパスワードを入力します。

ステップ 12 ［サービス機能（Service Capabilities）］で、［**サードパーティのメッセージ ストア内の電子メールへのユーザ アクセス（User Access to Email in Third-Party Message Store）**］チェックボックスをオンにします。

ステップ 13 ［**保存（Save）**］をクリックします。

ステップ 14 ライセンスのある Connection ユーザにアクセスを許可する電子メールが保持されたこの他の Exchange サーバごとに、ステップ 2 ～ステップ 13 を繰り返します。

ステップ 15 Cisco Unity Connection の管理を閉じます。

外部サービス用のユーザの設定

次の手順を実行します。

（注） Exchange は、設定する Connection ユーザごとにユーザを必要とします。

外部サービス用にユーザを設定する

ステップ 1 Cisco Unity Connection の管理で、［**(ユーザ（Users）**］を展開し、［**ユーザ（Users）**］をクリックします。

ステップ 2 ［ユーザの検索（Search Users）］ページで、ユーザのエイリアスをクリックします。

ステップ 3 ［ユーザの基本設定の編集（Edit User Basics）］ページで、［編集（Edit）］メニューの［**外部サービスのアカウント（External Service Accounts）**］をクリックします。

ステップ 4 ［外部サービスのアカウント（External Service Accounts）］ページで、［**新規追加（Add New）**］をクリックします。

ステップ 5 ［外部サービスのアカウントの新規作成（New External Service Accounts）］ページの［外部サービス（External Service）］フィールドで、P.40-19 の「ユーザがアクセスできる Exchange サーバを指定するための Cisco Unity Connection 外部サービスの作成」で作成した適切な外部サービスの表示名をクリックします。

ステップ 6 ［電子メール（Email Address）］フィールドに、ユーザの電子メール アドレスを入力します。

ステップ 7 ［ログイン タイプ（Login Type）］フィールドで、次の適切なオプションをクリックします。

- ［**接続エイリアスを使用（Use Connection Alias）**］：このオプションは、Exchange 2003 の［ユーザー ID］設定が Connection ユーザ エイリアスと同一である場合に便利です。Connection は、Connection ユーザ エイリアスを使用してユーザをログインさせます。
- ［**次のユーザ ID を使用：（Use User ID Provided Below）**］：Exchange 2003 の［ユーザー ID］設定を入力します（［ユーザー ID］設定が Connection ユーザ エイリアスと異なる場合に便利です）。Connection は、このフィールドの設定を使用してユーザをログインさせます。

ステップ 8　*（ステップ 7 で［次のユーザ ID を使用：（Use User ID Provided Below）］オプションを選択した場合のみ）*［ユーザ ID（User ID）］フィールドに、Exchange の［ユーザー ID］設定を入力します。

ステップ 9　［サービス機能（Service Capabilities）］で、**［サードパーティのメッセージ ストア内の電子メールへのユーザ アクセス（User Access to Email in Third-Party Message Store）］**チェックボックスをオンにします。

ステップ 10　**［保存（Save）］**をクリックします。

ステップ 11　ユーザの Exchange 設定を確認するには、**［テスト（Test）］**をクリックします。［タスクの実行結果（Task Execution Results）］ウィンドウにテスト結果が表示されます。

テストのいずれかの部分が失敗した場合は、Exchange、Cisco Unity Connection、およびユーザの設定を確認します。

ステップ 12　残りすべてのユーザについて、ステップ 2 ～ステップ 11 を繰り返します。