CHAPTER 33

パーソナル着信転送ルールで使用するための Exchange 予定表と連絡先へのアクセスの設定

Cisco Unity パーソナル着信転送ルール機能を使用できるサービス クラスに所属しているユーザについては、各自の Outlook 予定表と連絡先にアクセスできるように設定することもできます。このように設定すると、発信者に基づいて、および各自の予定表の予定に基づいて Connection ユーザがルールを作成できるようになります。この章では、Exchange と Cisco Unity Connection を設定して、Exchange の予定表と連絡先の情報を使用してユーザがパーソナル着信転送ルールを作成できるようにします。

次の各項を参照してください。

予定表と連絡先へのアクセスを許可してパーソナル着信転送ルールに使用できるようにするためのタスク リスト

ユーザが Outlook の予定表と連絡先にアクセスしてパーソナル着信転送ルールに使用することを許可するには、次の作業を記述されている順序どおりに実行します。

1. ユーザまたはテンプレートが、Cisco Unity パーソナル着信転送ルール機能を使用できるサービス クラスに関連付けられていることを確認します。
2. Exchange の予定表と連絡先へのアクセスを設定します。
   a. ユーザのアクセスするすべての Exchange 予定表と連絡先が Exchange 2007 に配置されている場合は、ステップ c. に進みます。

      ユーザのアクセスする Exchange 予定表と連絡先のいずれかが Exchange 2000 または Exchange 2003 に配置されている場合は、Exchange データへのアクセスで Connection が使用する Active Directory サービス アカウントを作成します。P.33-3 の「Active Directory サービス アカウントの作成（Exchange 2000 および Exchange 2003 のみ）」を参照してください。
   b. ユーザのアクセスする Exchange 予定表と連絡先のいずれかが Exchange 2000 または Exchange 2003 に配置されている場合は、必要な権限をサービス アカウントに付与します。P.33-4 の「サービス アカウントへの Exchange 権限の付与（Exchange 2000 および Exchange 2003 のみ）」を参照してください。
   c. アクセスする予定表と連絡先のデータが保持された各 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.33-6 の「SSL 証明書の作成とインストール」を参照してください。
   d. Connection 外部サービスを作成します。P.33-16 の「ユーザがアクセスできる Exchange サーバを指定するための Connection 外部サービスの作成」を参照してください。
   e. 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.33-18 の「Exchange 証明書を信頼するための Cisco Unity Connection サーバの設定」を参照してください。
   f. 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受け入れないように IIS を設定します。P.33-20 の「Connection と Exchange サーバ間での安全な通信の要求（省略可能、ただし推奨）」を参照してください。
   g. NTP サーバにアクセスするように Connection サーバを設定します。P.33-22 の「Cisco Unity Connection サーバと Exchange サーバのクロックの同期化」を参照してください。
3. 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。このアカウントを作成すると、ユーザがパーソナル着信転送ルール Web ツールを使用するときに、各自の予定表と連絡先にアクセスできるようになります。『*Cisco Unity Connection ユーザの移動、追加、変更 ガイド*』の「ユーザ アカウントの設定によって制御される機能の設定」の章の「パーソナル着信転送ルールに使用するための Exchange 予定表および連絡先へのアクセス」の項を参照してください。このドキュメントは、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html から入手可能です。
4. Outlook の予定表と連絡先にアクセスしてパーソナル着信転送ルールで使用する方法をユーザに通知するには、『*Cisco Unity Connection ユーザ ガイド*』の「着信を処理するパーソナル着信転送ルールの管理」および「個人連絡先リストの管理」の章を参照してもらいます。このドキュメントは、http://www.cisco.com/en/US/products/ps6509/products_user_guide_list.html から入手可能です。

Active Directory サービス アカウントの作成（Exchange 2000 および 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 2000 および Exchange 2003 の予定表と連絡先データにアクセスします。サービス アカウントを作成するには、次の手順を実行します。

Cisco Unity Connection が Exchange データへのアクセスに使用する AD サービス アカウントを作成する

ステップ 1　［Active Directory ユーザーとコンピュータ］がインストールされたサーバ上で、ユーザを新規作成する権限の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］>［Active Directory ユーザーとコンピュータ］**をクリックします。または、**［プログラム］>［管理ツール］>［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、アカウントを作成するドメインを展開して［**Users**］を右クリックするか、アカウントを作成する組織ユニットを右クリックして、**［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、サービス アカウントを作成します。オプションは次のように選択します。

- パスワード オプションを選択するときは、パスワードが期限切れにならないオプションを選択します。パスワードの有効期限が切れた場合、Connection は次にサーバが再起動された時点で動作を停止します。
- Exchange メールボックスは作成しないでください。

ステップ 5　［Active Directory ユーザーとコンピュータ］を閉じます。

サービス アカウントへの Exchange 権限の付与（Exchange 2000 および Exchange 2003 のみ）

Active Directory サービス アカウントが Exchange 2000 と Exchange 2003 のデータにアクセスできるようにするには、［Exchange 管理者 (参照のみ可)］制御をアカウントに委任し、［Administer information store］、［Send As］、および［Receive As］の各権限を付与します。

制御の委任は、組織レベルと管理グループ レベルのどちらでも実施できます。管理グループ レベルで制御を委任する場合は、次のメールストアを保持しているすべての管理グループで制御を委任する必要があります。

- Connection ユーザが連絡先のインポート元として使用する Exchange メールストア。
- Connection が Exchange 予定表データにアクセスできる Exchange メールストア。

Exchange の権限をサービス アカウントに付与する

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　Exchange システム マネージャの左ペインで、ツリー コントロールの最上位にある組織名を右クリックするか、アクセスする予定表と連絡先データのあるメールストアが保持された管理グループを右クリックして、**［制御の委任］**をクリックします。

ステップ 4　［Exchange 管理委任ウィザードへようこそ］ページで、**［次へ］**をクリックします。

ステップ 5　［ユーザまたはグループ］ダイアログボックスで、**［追加］**をクリックします。

ステップ 6　［制御の委任］ダイアログボックスで、**［参照］**をクリックします。

ステップ 7　サービス アカウントの名前を指定します。Exchange のバージョンによって手順が異なります。

Exchange 2003	**a.** ［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で、［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 P.33-3 の手順「Cisco Unity Connection が Exchange データへのアクセスに使用する AD サービス アカウントを作成する」で作成したアカウントのユーザ ログイン名を入力します。 **b.** **［名前の確認］**をクリックします。 **c.** **［OK］**をクリックして［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を閉じます。選択したアカウントが［グループ (推奨) またはユーザー］ボックスに表示されます。
Exchange 2000	**a.** ［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［場所］リストで、P.33-3 の手順「Cisco Unity Connection が Exchange データへのアクセスに使用する AD サービス アカウントを作成する」でアカウントを作成したドメインの名前をクリックします。 **b.** ユーザ、コンピュータ、およびグループのリストで、サービス アカウントの名前をダブルクリックします。 ［制御の委任］ダイアログボックスが再度表示されます。選択したアカウントが［グループ (推奨) またはユーザー］ボックスに表示されます。

ステップ 8　［役割］リストで、**［Exchange 管理者（参照のみ可）］**をクリックします。

ステップ 9　**［OK］**をクリックして［制御の委任］ダイアログボックスを閉じます。

ステップ 10　**［次へ］**をクリックします。

ステップ 11　**［完了］**をクリックします。

ステップ 12　ステップ 3 で、ツリー コントロールの最上位にある組織名を選択した場合はステップ 13 に進みます。

ステップ 3 で管理グループを選択した場合、この他の管理グループのメールストアに含まれている予定表と連絡先のデータにアクセスする必要があるときは、管理グループごとにステップ 3 ～ステップ 11 を繰り返します。

ステップ 13　Exchange システム マネージャの左ペインで、アクセスする予定表と連絡先データのあるメールボックスが保持されたメールボックス ストア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 14　［< 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 15　**［追加］**をクリックします。

ステップ 16　サービス アカウントの名前を指定します。Exchange のバージョンによって手順が異なります。

Exchange 2003	**a.** ［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、サービス アカウントの名前を入力します。 **b.** **［名前の確認］**をクリックします。
Exchange 2000	**a.** ［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［場所］リストで、サービス アカウントを作成したドメインの名前をクリックします。 **b.** ユーザ、コンピュータ、およびグループのリストで、サービス アカウントの名前をダブルクリックします。 ［制御の委任］ダイアログボックスが再度表示されます。選択したアカウントが［グループ (推奨) またはユーザー］ボックスに表示されます。

ステップ 17　**［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 18　［メールボックス ストア < 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 19　［< アカウント名 > のアクセス許可］リストの［許可］カラムで、次の 3 つのチェックボックスをオンにします。

- ［Administer information store］
- ［Receive As］
- ［Send As］

この他の権限は変更しないでください。

ステップ 20　［OK］をクリックして［メールボックス ストア < 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 21　アクセスする Exchange データが保持されているこの他の Exchange サーバごとに、ステップ 13 ～ ステップ 20 を繰り返します。

ステップ 22　Exchange システム マネージャを閉じます。

SSL 証明書の作成とインストール

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予定表と連絡先が保持された各 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、サービス アカウントの資格情報（Exchange 2000 または Exchange 2003）または個々のユーザの資格情報（Exchange 2007）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 が予定表と連絡先のデータ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。

SSL 証明書を作成し、インストールして、Exchange 予定表と連絡先への Cisco Unity Connection のアクセスをセキュリティで保護するには、次の作業を行います。

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。P.33-7 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」を参照してください。

   この他のアプリケーションを使用して SSL 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。インストール手順については、製造元のマニュアルを参照してください。次に、ステップ 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、ステップ 2. に進みます。

2. 証明書署名要求を作成し、証明書を発行してインストールします。
   - アクセスする予定表と連絡先のデータが保持された Exchange サーバごとに、証明書署名要求を作成します。
   - 証明書署名要求ごとに、外部の認証局に SSL 証明書を発行してもらうか、Microsoft 証明書サービス（または同等の機能を備えた他のアプリケーション）を使用して独自に証明書を発行します。
   - Exchange 2000 および Exchange 2003 の場合は、SSL 証明書をインストールします。Exchange 2007 の場合は、証明書をインポートして有効にします（Exchange 2007 でも目的は同じですが、用語が変更されました）。

   次の該当する項を参照してください。
   - 証明書署名要求の作成、および証明書の発行とインストール（Exchange 2000 および Exchange 2003 のみ）（P.33-8）
   - 証明書署名要求の作成、および証明書の発行、インポート、有効化（Exchange 2007 のみ）（P.33-12）

SSL 証明書を作成してインストールしていない場合でも、Connection はサービス アカウントの資格情報を暗号化された形式で送信することがあります。これは、Exchange で認証方式を 1 つまたはそれ以上設定したかどうかによって決まります。ただし、これらの使用可能な Exchange 認証方式で暗号化されるのは、ユーザ名とパスワードのみであり、予定表と連絡先のデータは暗号化されません。また、Exchange のドキュメントでは、これらの使用可能な認証方式を使用した場合、提供されるセキュリティ レベルが一定しないと記述されています。SSL 証明書を作成してインストールすることをお勧めします。

注意　Cisco Unity Connection は Passport 認証をサポートしていません。

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　メンバー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］コントロール パネルを閉じます。

証明書署名要求の作成、および証明書の発行とインストール（Exchange 2000 および Exchange 2003 のみ）

Exchange 2000 サーバおよび Exchange 2003 サーバの証明書署名要求を作成する

ステップ 1　Cisco Unity Connection ユーザの Exchange 予定表と連絡先が保持された Exchange 2000 サーバまたは Exchange 2003 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］>［インターネット インフォメーション サービス（IIS）マネージャ］**をクリックします。

ステップ 3　サーバが Windows Server 2003 を実行している場合は、Windows の［スタート］メニューで、**［プログラム］>［管理ツール］>［インターネット インフォメーション サービス (IIS) マネージャ］**をクリックします。

サーバが Windows 2000 Server を実行している場合は、Windows の［スタート］メニューで、**［プログラム］>［管理ツール］>［インターネット サービス マネージャ］**をクリックします。

ステップ 4　インターネット インフォメーション サービスの左ペインで、この Exchange サーバの名前を展開します。

ステップ 5　サーバが Windows 2000 Server を実行している場合は、ステップ 6 に進みます。

サーバが Windows Server 2003 を実行している場合は、**［Web サイト］**を展開します。

ステップ 6　**［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 7　［既定の Web サイトのプロパティ］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 8　［セキュリティ保護された通信］の**［サーバ証明書］**をクリックします。

ステップ 9　［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 10　**［証明書の新規作成］**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　**［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 13　**［次へ］**をクリックします。

ステップ 14　証明書の名前を入力し、デフォルトのビット長をそのまま使用します。

ステップ 15　**［次へ］**をクリックします。

ステップ 16　組織に関する情報を入力します。

ステップ 17　**［次へ］**をクリックします。

ステップ 18 サイトの一般名に、Exchange サーバのコンピュータ名または完全修飾ドメイン名のいずれかを入力します。

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 19［次へ］をクリックします。

ステップ 20［地理情報］ページで、適切な情報を入力します。

ステップ 21［次へ］をクリックします。

ステップ 22［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.33-7 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 23［次へ］をクリックします。

ステップ 24［要求ファイルの概要］ページで、要求ファイルに関する情報を確認します。

ステップ 25［次へ］をクリックします。

ステップ 26［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 27［OK］をクリックして［既定の Web サイトのプロパティ］ダイアログボックスを閉じます。

ステップ 28 インターネット インフォメーション サービス マネージャを閉じます。

ステップ 29 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 30 Connection ユーザにアクセスを許可する予定表と連絡先データ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 29 を繰り返して証明書署名要求を作成します。

ステップ 31 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、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.33-11 の手順「Exchange 2000 サーバおよび Exchange 2003 サーバに証明書をインストールする」に進みます。

P.33-8 の手順「Exchange 2000 サーバおよび Exchange 2003 サーバの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 形式で発行します。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.33-11 の手順「Exchange 2000 サーバおよび Exchange 2003 サーバに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.33-11 の手順「Exchange 2000 サーバおよび Exchange 2003 サーバに証明書をインストールする」に進みます。

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.33-7 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.33-8 の手順「Exchange 2000 サーバおよび Exchange 2003 サーバの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、**［開く］**をクリックします。

ステップ 10　［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 11　**［ファイルにコピー］**をクリックします。

ステップ 12　［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 13　［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 14　**［次へ］**をクリックします。

ステップ 15　［エクスポートするファイル］ページで、**［参照］**をクリックします。

ステップ 16［名前を付けて保存］ダイアログボックスで、場所を選択してファイル名を入力します。

このサーバにインターネット インフォメーション サービス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 17 この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 18［**保存**］をクリックして［名前を付けて保存］ダイアログボックスを閉じます。

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 21［**OK**］をクリックして、正しくエクスポートされたことを示すメッセージをクリアします。

ステップ 22［**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 23 P.33-8 の手順「Exchange 2000 サーバおよび Exchange 2003 サーバの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 22 を繰り返します。

ステップ 24［証明機関］を閉じます。

ステップ 25 インターネット インフォメーション サービス 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。

Connection ユーザにアクセスを許可する予定表と連絡先のデータが保持されたすべての Exchange 2000 または Exchange 2003 サーバで、次の手順を実行します。

Exchange 2000 サーバおよび Exchange 2003 サーバに証明書をインストールする

ステップ 1 SSL 証明書のあるいずれかの Exchange 2000 サーバまたは Exchange 2003 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**］>［**インターネット インフォメーション サービス（IIS）マネージャ**］をクリックします。

ステップ 3 左ペインで、この Exchange サーバの名前を展開します。

ステップ 4［**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 5［既定の Web サイトのプロパティ］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 6［セキュリティ保護された通信］の［**サーバ証明書**］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　［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　［証明書の概要］ページで、証明書に関する情報を確認します。

ステップ 12　**［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］**をクリックして Web サーバ証明書ウィザードを終了します。

ステップ 14　**［OK］**をクリックして［既定の Web サイトのプロパティ］ダイアログボックスを閉じます。

ステップ 15　IIS を再起動します。

a. インターネット インフォメーション サービス マネージャの左ペインで、この Exchange サーバの名前を右クリックし、**［IIS の再起動］**をクリックします。
b. ［停止 / 開始 / 再起動］ダイアログボックスで、**［< サーバ名 > のインターネット サービスを再起動します］**をクリックします。
c. **［OK］**をクリックします。
d. インターネット インフォメーション サービス マネージャを閉じます。

ステップ 16　インストールする証明書ごとに、ステップ 1 ～ステップ 15 を繰り返します。

証明書署名要求の作成、および証明書の発行、インポート、有効化（Exchange 2007 のみ）

Exchange 2007 サーバで証明書署名要求を作成する

ステップ 1　Cisco Unity Connection ユーザの Exchange 予定表と連絡先データが保持された Exchange 2007 サーバ上で、Exchange 管理シェルの New-ExchangeCertificate コマンドを実行するために必要な権限の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 Server 2007］**>**［Exchange 管理シェル］**をクリックします。

ステップ 3　次のコマンドを実行します。

New-ExchangeCertificate -GenerateRequest -DomainName < ドメイン名 >
-PrivateKeyExportable $true -path < 証明書署名要求のパスとファイル名 >

ステップ 4　Exchange 管理シェルを閉じます。

ステップ 5　この他の Exchange 2007 サーバにある予定表と連絡先のデータにアクセスする必要がある場合は、アクセスするデータを保持しているサーバごとに、ステップ 1 ～ステップ 4 を繰り返します。

P.33-12 の手順「Exchange 2007 サーバで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、サーバ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。信頼する証明書を発行するときは、.pem ファイル名拡張子の付いた Base-64 符号化 X.509 形式で発行します。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.33-14 の手順「Exchange 2007 サーバ上で SSL 証明書をインポートして有効にする」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発行するように要求します。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.33-14 の手順「Exchange 2007 サーバ上で SSL 証明書をインポートして有効にする」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.33-7 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.33-12 の手順「Exchange 2007 サーバで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、**［開く］**をクリックします。

ステップ 10　［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 11　**［ファイルにコピー］**をクリックします。

ステップ 12［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 13［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 14［次へ］をクリックします。

ステップ 15［エクスポートするファイル］ページで、**［参照］**をクリックします。

ステップ 16［名前を付けて保存］ダイアログボックスで、場所を選択してファイル名を入力します。

このサーバにインターネット インフォメーション サービス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 17 この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 18［保存］をクリックして［名前を付けて保存］ダイアログボックスを閉じます。

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 21［OK］をクリックして、正しくエクスポートされたことを示すメッセージをクリアします。

ステップ 22［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 23 P.33-12 の手順「Exchange 2007 サーバで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 22 を繰り返します。

ステップ 24［証明機関］を閉じます。

ステップ 25 インターネット インフォメーション サービス 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。

Connection ユーザにアクセスを許可する予定表と連絡先のデータが保持されたすべての Exchange 2007 サーバで、次の手順を実行します。

Exchange 2007 サーバ上で SSL 証明書をインポートして有効にする

ステップ 1 SSL 証明書のあるサーバ上で、Exchange 管理シェルの Import-ExchangeCertificate コマンドおよび Enable-ExchangeCertificate コマンドを実行するために必要な権限の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 Server 2007］**>**［Exchange 管理シェル］**をクリックします。

ステップ 3　次のコマンドを実行します。

Import-ExchangeCertificate -path < 証明書のパスとファイル名 >

ステップ 4　Import-ExchangeCertificate コマンドで表示されたフィンガープリントを Windows クリップボードにコピーします。

ステップ 5　Exchange 管理シェルで、次のコマンドを実行します。

Enable-ExchangeCertificate -Thumbprint < ステップ 4 でコピーしたフィンガープリント > -Services IIS

ステップ 6　Exchange 管理シェルを閉じます。

ステップ 7　P.33-12 の手順「Exchange 2007 サーバで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、SSL 証明書のある Exchange 2007 サーバごとに、ステップ 1 ～ステップ 6 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 Connection 外部サービスの作成

Cisco Unity Connection の管理で、Connection ユーザにアクセスを許可する予定表と連絡先のデータが保持された Exchange サーバごとに 1 つずつ、［予定表と個人連絡先］外部サービスを作成し、設定します。

ユーザがアクセスできる Exchange サーバを指定するための Connection 外部サービスを作成する

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　**［新規追加（Add New）］**をクリックします。

ステップ 3　［タイプ（Type）］リストで、**［予定表と個人連絡先（Calendar and Personal Contacts）］**をクリックします。

ステップ 4　各自の予定表と連絡先情報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予定表と連絡先のデータが保持された Exchange サーバの名前を含めます）。

ステップ 5　［サーバ ベース URL（Server Base URL）］フィールドに、Connection ユーザにアクセスを許可する予定表と連絡先のデータが保持された Exchange サーバの URL を入力します。**https://<Exchange サーバ >/Exchange/** 形式を使用してください。<Exchange サーバ > は、Exchange サーバのコンピュータ名、完全修飾ドメイン名（FQDN）、または IP アドレスです。

Exchange 2000 サーバまたは Exchange 2003 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する場合、<Exchange サーバ > に入力する値は、P.33-8 の手順「Exchange 2000 サーバおよび Exchange 2003 サーバの証明書署名要求を作成する」のステップ 18 で入力した値と完全に一致している必要があります。

注意　**https** の代わりに **http** を入力して P.33-20 の「Connection と Exchange サーバ間での安全な通信の要求（省略可能、ただし推奨）」の手順を実行した場合、予定表と連絡先のデータを Exchange から Connection に転送しようとすると失敗します。**https** の代わりに **http** を入力して前述の項の手順を実行しない場合、予定表と連絡先のデータは、暗号化されないまま Exchange から Connection に転送されます。

ステップ 6　**［アクセスを可能にする（Access 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 7　Exchange 2007 サーバにアクセスする場合：

a. ［サービス クレデンシャルを使用する（Use Service Credentials）］チェックボックスをオフにします。

b. ステップ 8 に進みます。

Exchange 2000 サーバまたは Exchange 2003 サーバにアクセスする場合：

a. ［サービス クレデンシャルを使用する（Use Service Credentials）］チェックボックスをオンにします。

b. ［サービス ログイン（Service Login）］フィールドに、P.33-3 の手順「Cisco Unity Connection が Exchange データへのアクセスに使用する AD サービス アカウントを作成する」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。

   < ドメイン名 > と < アカウント名 > の間に円記号（\）があることに注意してください。スラッシュ（/）を使用した場合、［予定表と個人連絡先］サービスは機能しません。

c. ［サービス パスワード（Service 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 8　**［保存（Save）］**をクリックします。

ステップ 9　ユーザにアクセスを許可するすべての Exchange サーバについて外部サービスを設定した場合、この手順の残りの部分に進みます。

この他の Exchange サーバにユーザがアクセスできるようにする場合は、［外部サービス（External Service）］メニューの**［外部サービスの新規作成（New External Service）］**をクリックします。

ステップ 10　必要な外部サービスをすべて作成するまで、ステップ 3 ～ステップ 9 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 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。

Connection と Exchange サーバ間での安全な通信の要求（省略可能、ただし推奨）

この章のこれまでの手順のいくつかは、Exchange から Cisco Unity Connection に転送される予定表と連絡先のデータを暗号化によって保護するのに役立ちます。ただし、P.33-16 の「ユーザがアクセスできる Exchange サーバを指定するための Connection 外部サービスの作成」の手順を実行したときに https URL ではなく http URL を指定した場合は、データが暗号化されないままネットワーク経由で送信されます。

各 Exchange サーバ上で、次の手順を実行することをお勧めします。この手順を完了すると、ユーザのアクセスできる Exchange サーバのリストを Connection 管理者が更新するときに、誤って http URL を指定した場合、暗号化されていない Exchange データを転送しようとした時点で処理が失敗します。

注意　これはグローバル設定です。この手順を実行した Exchange サーバは、そのサーバ上の Exchange データにアクセスするすべての Web クライアントに対して、https URL を使用するように要求します。

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

ステップ 1　Exchange データにアクセスする Web クライアントに対して https URL の使用を要求するようにインターネット インフォメーション サービスを設定した場合でも、他のアプリケーションに影響がないことを確認します。

ステップ 2　Connection ユーザが予定表または連絡先のインポート元として使用するメールボックスが保持された Exchange サーバにログインします。

ステップ 3　サーバが Windows Server 2003 を実行している場合は、Windows の［スタート］メニューで、**［プログラム］>［管理ツール］>［インターネット インフォメーション サービス (IIS) マネージャ］**をクリックします。

サーバが Windows 2000 Server を実行している場合は、Windows の［スタート］メニューで、**［プログラム］>［管理ツール］>［インターネット サービス マネージャ］**をクリックします。

ステップ 4　インターネット インフォメーション サービスの左ペインで、この Exchange サーバの名前を展開します。

ステップ 5　サーバが Windows 2000 Server を実行している場合は、ステップ 6 に進みます。

サーバが Windows Server 2003 を実行している場合は、**［Web サイト］**を展開します。

ステップ 6　**［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 7　［既定の Web サイトのプロパティ］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 8　［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 9　［セキュリティ保護された通信］ダイアログボックスで、**［保護されたチャンネル (SSL) を要求する］**チェックボックスをオンにします。

ステップ 10　**［OK］**をクリックして［セキュリティ保護された通信］ダイアログボックスを閉じます。

ステップ 11　**［OK］**をクリックして［既定の Web サイトのプロパティ］ダイアログボックスを閉じます。

ステップ 12　インターネット インフォメーション サービスを閉じます。

ステップ 13　子ノードについてこの設定をオンにするように求められた場合は、この設定を有効にする子ノードを選択し、**［OK］**をクリックします。

ステップ 14　Cisco Unity Connection ユーザが予定表または連絡先データのインポート元として使用するメールボックスが保持された各 Exchange サーバ上で、ステップ 1 ～ステップ 13 を繰り返します。

Cisco Unity Connection サーバと Exchange サーバのクロックの同期化

予定表データに基づいたパーソナル着信転送ルールを使用する場合は、Cisco Unity Connection サーバと、Connection が予定表データにアクセスするすべての Exchange サーバでシステム クロックが同期化されている必要があります。

注意　Connection サーバ上の時刻が、予定表データがアクセスされる Exchange サーバ上の時刻と一致していない場合、予定表データに基づいたパーソナル着信転送ルールによって着信が正しく転送されません。

NTP サーバにアクセスするように Cisco Unity Connection サーバと Exchange サーバを設定する

ステップ 1　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 2　［設定（Settings）］メニューの［**NTP サーバ（NTP Servers）**］をクリックします。

ステップ 3　［**新規追加（Add New）**］をクリックします。

ステップ 4　［**ホスト名または IP アドレス（Hostname or IP Address）**］フィールドに、NTP サーバの DNS 名（FQDN）または IP アドレスを入力します。このホスト名または IP アドレスは、Connection サーバ、および Connection のアクセスする予定表データが保持されたすべての Exchange サーバが解決できる必要があります。

ステップ 5　［**保存（Save）**］をクリックします。

ステップ 6　Connection のアクセスする予定表データが保持されたすべての Exchange サーバを、ステップ 4 で Cisco Unity Connection サーバに対して選択した同じ NTP サーバとクロックが同期化されるように設定します。

詳細については、Microsoft の Web サイトを参照してください。