CHAPTER 20

IMAP 設定値の設定

この章では、ユーザが IMAP クライアントを使用して Connection サーバ経由でメッセージの送信、転送、または返信を行うことができるように Cisco Unity Connection を設定する方法について説明します。

次の各項を参照してください。

SMTP メッセージ処理の概要

Cisco Unity Connection は、IMAP クライアントによって生成された SMTP メッセージを受信して処理できます。たとえば、ViewMail for Outlook を使用して Microsoft Outlook 電子メール クライアントで録音したボイス メッセージなどの受信と処理を行えます。

認証済みの IMAP クライアントが SMTP を介して Connection へのメッセージの送信を試行すると、Connection はメッセージをボイスメール、電子メール、ファックス、または送信確認として分類することを試みます。また、Connection は、メッセージのヘッダーにある SMTP アドレスと SMTP プロキシ アドレスのリストを比較して、送信者とユーザとのマッピング、およびメッセージの受信者とユーザや連絡先とのマッピングを試みます。

SMTP 認証が IMAP クライアントに対して設定されており、送信者の SMTP アドレスが認証済みユーザのプロキシ アドレスまたはプライマリ SMTP アドレスと一致する場合、または SMTP 認証が IMAP クライアントに対して設定されておらず、送信者の SMTP アドレスがいずれかの Connection ユーザのプロキシ アドレスまたはプライマリ SMTP アドレスに一致する場合、Connection は、受信者のタイプに基づいてそれぞれの受信者ごとに次のようにメッセージを処理します。

- 受信者が VPIM 連絡先にマッピングされた場合、Connection はメッセージを VPIM メッセージに変換し、VPIM 標準で許可されていない添付ファイルをすべて削除します。次に、Connection は、指定された VPIM ロケーションのホームがローカル サーバである場合には、その VPIM ロケーションにメッセージを送信し、VPIM ロケーションのホームがデジタル ネットワークで接続された別の Connection サーバである場合には、そのサーバにメッセージを転送します。
- 受信者が、ローカル　サーバをホームとするユーザにマッピングされた場合、Connection　は、Cisco Unity Connection の管理にあるそのユーザのプロファイルの［メッセージアクション（Message Actions）］ページで指定されているアクションを実行します。メッセージのタイプ（ボイス、電子メール、ファックス、または送信確認）ごとに、Connection がメッセージを受け入れて Connection サーバ上のユーザのメールボックスに配置するか、代行 SMTP アドレスでユーザにメッセージをリレーするか、メッセージを拒否して不達確認（NDR）を生成するかを設定できます。
- 受信者が、リモート Connection サーバをホームとするユーザにマッピングされた場合、Connection はユーザのホーム サーバにメッセージをリレーします。その結果、ホーム サーバが、ユーザ プロファイルの［メッセージアクション（Message Actions）］ページで指定されているアクションを実行します。
- 受信者が上記のいずれにもマッピングされない場合、Connection は、メッセージを SMTP スマート ホストにリレーするか、NDR を送信者に送信します。これは、Connection の管理の［システム設定（System Settings）］>［全般的な設定（General Configuration）］ページにある［受信者が見つからない場合（When a recipient can not be found）］設定で選択されているオプションに応じて決定されます。デフォルトでは、Connection は NDR を送信します。

SMTP 認証が IMAP クライアントに対して設定されており、送信者の SMTP アドレスが認証済みユーザのプロキシ アドレスまたはプライマリ SMTP アドレスに一致しない場合、Connection サーバは SMTP エラーを返します。このため、ほとんどの場合、メッセージがクライアントのアウトボックスに残ることになります。SMTP 認証が IMAP クライアントに対して設定されておらず、送信者の SMTP アドレスが既知のユーザのプロキシ アドレスまたはプライマリ SMTP アドレスに一致しない場合、Connection はメッセージを MTA の不正メール フォルダ（UmssMtaBadMail）に配置します。

メッセージに安全なヘッダーが含まれている場合、またはメッセージの送信者が、常に安全なメッセージを送信するように設定されたサービス クラスに属するユーザである場合、Connection は着信 SMTP メッセージに安全のマークを付けます。安全なメッセージの受信および安全なメッセージへのアクセスが可能なユーザの詳細については、P.24-2 の「プライベートまたは安全のマークが付いたメッセージに対する Cisco Unity Connection の処理」を参照してください。

メッセージ アクション

Connection は、ユーザのメッセージ アクション設定に基づいて、ユーザ宛てのさまざまなタイプのメッセージを処理する方法を決定します。特定のタイプのメッセージ（ボイス、電子メール、ファックス、または送信確認）のメッセージ アクション設定は、クライアントから（電話インターフェイス、Cisco Unity Assistant、IMAP クライアントなどを使用して）Connection サーバに送信または作成されたそのタイプのメッセージすべてに影響します。

デフォルトでは、Connection は各タイプのメッセージを受け入れるように設定されています。これは、Connection が適切な Connection メールボックス ストア内のユーザ メールボックスにメッセージを配置するアクションです。

リレー アクションを使用すると、特定のタイプのすべてのメッセージを別のメッセージ システム（企業の電子メール サーバなど）に送信して、メッセージの保存とユーザ アクセスがそのメッセージ システムで行われるように Connection に指示できます。このオプションを選択した場合、ユーザはそれらのタイプのメッセージに対して、Connection 電話インターフェイス、Cisco Unity Assistant、または Phone View や Cisco Unified Personal Communicator などのその他のクライアントからアクセスすることができなくなります（ただし、ユーザが電話で Connection にログオンしたときに電子メールが読み上げられるように、Connection で接続先として設定されている外部メッセージ ストアに電子メール メッセージをリレーすることは例外です）。1 つまたは複数のメッセージ アクションを設定して、メッセージをユーザの単一の SMTP リレー アドレスにリレーします。これは、ユーザの［メッセージアクション（Message Actions）］ページで定義します（また、ユーザ テンプレートに対してメッセージ アクションを設定することや、一括編集ユーティリティで複数のユーザに対して一度にメッセージ アクションを設定することもできます。この場合は、テキストと置換可能なトークンの組み合せを使用して SMTP アドレス用のテンプレートを定義します。このテンプレートから、Connection が個々のユーザのリレー アドレスを作成します）。Connection は SMTP スマート ホストを介してメッセージをリレーするため、ユーザやユーザ テンプレートにこのアクションを設定するには、Connection サーバ上にスマート ホストを設定する必要があります。

拒否アクションを使用すると、ユーザが受信する特定のタイプのメッセージをすべて削除し、メッセージの送信者に不達確認を送信するように Connection に指示できます。

IMAP アクセスの導入に関する推奨事項

IMAP クライアントを配置して Cisco Unity Connection メッセージへのアクセスやメッセージの送信を行う場合は、次の推奨事項を考慮してください。

- ファイアウォールを使用して、Connection SMTP ポートを不正アクセスから保護してください。SMTP のポートとドメインは、Cisco Unity Connection の管理の［システム設定（System Settings）］>［SMTP の設定（SMTP Configuration）］>［サーバ（Server）］ページに表示されます。
- ユーザのパスワードを保護するには、IMAP クライアント接続に対して Transport Layer Security（TLS; トランスポート層セキュリティ）を設定してください。
- ViewMail for Outlook は、ユーザが到達できるメッセージ受信者をそのユーザのサーチ スペース内のオブジェクトに制限しており、サーチ スペースに表示されない受信者に送信されたメッセージに対しては不達確認（NDR）を送信します。ユーザが到達できるオブジェクトを制限するためにサーチ スペースを使用している場合に、到達不能なオブジェクトの NDR をユーザが受信しないようにするには、ユーザ サーチ スペース内のオブジェクトに制限されている ViewMail ユーザ用に別の Outlook アドレス帳を作成することを検討してください。

Cisco Unity Connection で IMAP アクセスを設定するためのタスク リスト

1. *ユーザへのメッセージを別の SMTP サーバにリレーするように Cisco Unity Connection を設定する場合は、次のサブタスクを実行します。*
   a. Connection サーバからのメッセージを受け入れるように SMTP スマート ホストを設定します。ご使用の SMTP サーバ アプリケーションのドキュメントを参照してください。
   b. メッセージをスマート ホストにリレーするように Connection サーバを設定します。P.20-5 の「メッセージをスマート ホストにリレーするための Cisco Unity Connection サーバの設定」を参照してください。
2. Connection ユーザまたはユーザ テンプレートに対してメッセージ アクションを設定します。『*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「メッセージ アクション」の項を参照してください。
3. IMAP クライアントを使用してメッセージを送信または受信するユーザに対して、SMTP プロキシ アドレスを設定します。『*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「SMTP プロキシ アドレス」の項を参照してください。
4. IMAP クライアントを使用してボイス メッセージ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、ユーザを割り当てます。『*Cisco Unity Connection ユーザの移動、追加、変更 ガイド*』の「サービス クラスによって制御される機能の設定」の章の「ボイス メッセージへの IMAP クライアント アクセス」の項を参照してください。
5. IMAP クライアントを使用してメッセージを受信する VPIM 連絡先に対して、SMTP プロキシ アドレスを設定します。『*Cisco Unity Connection ユーザの移動、追加、変更 ガイド*』の「連絡先の管理」の章の「SMTP プロキシ アドレス」の項を参照してください。
6. IMAP クライアントからの SMTP 接続を許可するように Connection サーバを設定します。P.20-5 の「IMAP クライアントのアクセスおよび認証のための Cisco Unity Connection サーバの設定」を参照してください。
7. *タスク 6.* の手順でトランスポート層セキュリティ（TLS）を必須またはオプションに設定した場合：安全な IMAP 接続を提供するように Connection サーバを設定します。P.25-3 の「SSL サーバ証明書の作成とインストール」を参照してください。
8. オプションで、Connection が受け入れる SMTP メッセージの特性を指定する設定を変更します。P.20-7 の「SMTP メッセージのパラメータの設定」を参照してください。
9. ユーザのワークステーションごとに、サポートされている IMAP クライアントを Connection メールボックスにアクセスするように設定します。『*Cisco Unity Connection ユーザワークステーション セットアップ ガイド*』の「Cisco Unity Connection ボイス メッセージにアクセスするための電子メール アカウントの設定」の章を参照してください。

Cisco Unity Connection での IMAP アクセスの設定手順

メッセージをスマート ホストにリレーするための Cisco Unity Connection サーバの設定

どのタイプのメッセージでも、Cisco Unity Connection がメッセージをユーザの SMTP アドレスにリレーできるようにするには、スマート ホストを介してメッセージをリレーするように Connection サーバを設定する必要があります。

メッセージをスマート ホストにリレーするように Cisco Unity Connection サーバを設定する

ステップ 1　Cisco Unity Connection の管理で、［**システム設定（System Settings）**］を展開し、［**SMTP の設定（SMTP Configuration）**］を展開して、［**スマート ホスト（Smart Host）**］をクリックします。

ステップ 2　［**スマート ホスト（Smart Host）**］フィールドに、SMTP スマート ホスト サーバの IP アドレスまたは完全修飾ドメイン名を入力します（サーバの完全修飾ドメイン名を入力するのは、DNS が設定されている場合だけです）。

ステップ 3　［**保存（Save）**］をクリックします。

IMAP クライアントのアクセスおよび認証のための Cisco Unity Connection サーバの設定

Cisco Unity Connection との SMTP 接続を開始できるクライアントの種類を制御するためのオプションは多数あります。アクセス リストを作成し、そのアクセス リストを使用して、アクセスを許可または拒否するクライアントに対応する特定の IP アドレスまたは IP アドレス パターンを設定できます。また、IP アドレスにかかわらず、すべてのクライアントに対して接続を許可することもできます。そのようにした場合、それらのクライアント（信頼されていない IP アドレスと呼ばれる）が認証を受ける必要があるかどうか、また、信頼されていない IP アドレスを持つユーザに対してトランスポート層セキュリティ（TLS）を必須とするか許可するかを指定できます。

信頼されていない IP アドレスを持つクライアントに Connection での認証を要求することを選択した場合、ユーザは認証を受ける IMAP クライアントで、Connection エイリアスと Web アプリケーション（Cisco PCA）パスワードを入力します。Cisco Unity Assistant で Cisco PCA パスワードを変更するたびに、IMAP クライアントでもパスワードを更新しなければならないことをユーザが理解していることを確認してください。両方のアプリケーションで Cisco PCA パスワードを更新した後に IMAP クライアントでのボイス メッセージの受信に問題が発生した場合は、『*Cisco Unity Connection ユーザワークステーション セットアップ ガイド*』の「Cisco Unity Connection ボイス メッセージにアクセスするための電子メール アカウントの設定」の章の「IMAP クライアントのログオンに関する問題のトラブルシューティング」の項を参照してください。

必要に応じて、次のいずれかまたは両方の手順を実行します。

- Cisco Unity Connection IP アドレス アクセス リストを設定する（P.20-6）
- 信頼されていない IP アドレスに対してアクセスと認証を設定する（P.20-6）

Cisco Unity Connection IP アドレス アクセス リストを設定する

ステップ 1　Cisco Unity Connection の管理で、**［システム設定（System Settings）］**>**［SMTP の設定（SMTP Configuration）］**を展開して、**［サーバ（Server）］**をクリックします。

ステップ 2　［編集（Edit）］メニューで、**［IP アドレス アクセス リストの検索（Search IP Address Access List）］**をクリックします。

ステップ 3　新しい IP アドレスをリストに追加するには、**［新規追加（Add New）］**をクリックします。

ステップ 4　［アクセス IP アドレスの新規作成（New Access IP Address）］ページで、IP アドレスを入力します。または、1 つの *（アスタリスク）を入力して、対象となり得るすべての IP アドレスと一致させます。

ステップ 5　**［保存（Save）］**をクリックします。

ステップ 6　［アクセス IP アドレス（Access IP Address）］ページで、ステップ 4 で入力した IP アドレスからの接続を許可するために、**［接続を許可する（Allow Connection）］**チェックボックスをオンにします。この IP アドレスからの接続を拒否するには、このチェックボックスをオフにします。

ステップ 7　［アクセス IP アドレス（Access IP Address）］ページで変更を行った場合は、**［保存（Save）］**をクリックします。

ステップ 8　アクセス リストに追加する IP アドレスごとに、ステップ 2 ～ステップ 7 を繰り返します。

信頼されていない IP アドレスに対してアクセスと認証を設定する

ステップ 1　Cisco Unity Connection の管理で、**［システム設定（System Settings）］**>**［SMTP の設定（SMTP Configuration）］**を展開して、**［サーバ（Server）］**をクリックします。

ステップ 2　クライアントの IP アドレスからの接続を特別に許可するように Connection が設定されているかどうかにかかわらず、SMTP を使用して接続することをすべてのクライアントに許可するには、**［信頼されていない IP アドレスからの接続を許可する（Allow Connections From Untrusted IP Addresses）］**チェックボックスをオンにします。

ステップ 3　ステップ 2 でチェックボックスをオンにした場合、これらのタイプのクライアントに対して認証を設定するには、**［信頼されていない IP アドレスからの認証を要求する（Require Authentication From Untrusted IP Addresses）］**チェックボックスをオンにします。次に、信頼されていない IP アドレスに対して Connection がトランスポート層セキュリティ（TLS）をどのように処理するかを選択します。

- ［無効（Disabled）］: Connection は、信頼されていない IP アドレスを持つクライアントまたはサーバによって開始された SMTP セッションに対して、TLS をオプションとして提供しません。クライアントが TLS を使用するように設定されており、Connection が TLS を提供しない状況では、ほとんどの場合、接続は失敗し、クライアントがユーザに通知します。
- ［必須（Required）］: 信頼されていない IP アドレスから接続しているクライアントまたはサーバは、TLS を使用して Connection サーバとの SMTP セッションを開始する必要があります。
- ［オプション（Optional）］: 信頼されていない IP アドレスから接続しているクライアントまたはサーバは、TLS を使用して Connection との SMTP セッションを開始できますが、これは必須ではありません。

（注）　ユーザのパスワードを保護するためには、信頼されていない IP アドレスからの認証を要求し、トランスポート層セキュリティ（TLS）を［必須（Required）］または［オプション（Optional）］として設定することをお勧めします。

ステップ 4　ステップ 3 でトランスポート層セキュリティ（TLS）の設定に［必須（Required）］または［オプション（Optional）］を選択した場合は、Connection サーバに TLS を設定します。P.25-3 の「SSL サーバ証明書の作成とインストール」を参照してください。

SMTP メッセージのパラメータの設定

設定できる合計サイズより大きい着信 SMTP メッセージ、または設定できる受信者数より多く受信者を指定している着信 SMTP メッセージを拒否するように、Connection を設定できます。デフォルトでは、Connection は 10 MB より大きいメッセージ、または 15,000 人より多い受信者数を指定しているメッセージを受け入れます。

SMTP メッセージのパラメータを設定する

ステップ 1　Cisco Unity Connection の管理で、**［システム設定（System Settings）］**>**［SMTP の設定（SMTP Configuration）］**を展開して、**［サーバ（Server）］**をクリックします。

ステップ 2　SMTP クライアントによって送信される個々のメッセージのサイズを制限するには、キロバイト数を入力します。

ステップ 3　1 メッセージあたりの受信者数を制限するには、人数を入力します。

ステップ 4　このページのその他の設定を必要に応じて入力し、**［保存（Save）］**をクリックします。