CHAPTER 20

Cisco Unity Connection 8.x の IMAP 設定の構成

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。

次の項を参照してください。

Cisco Unity Connection 8.x の 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されたボイス メッセージなどを受信して処理できます。

認証済みの IMAP クライアントが SMTP を使用して Connection にメッセージを送信すると、Connection は、そのメッセージをボイスメール、電子メール、ファクス、または送信確認のいずれかに分類します。また、Connection は、メッセージのヘッダーにある SMTP アドレスを SMTP プロキシ アドレスのリストと比較して、メッセージの送信者をユーザにマッピングし、受信者をユーザまたは連絡先にマッピングします。

SMTP 認証が IMAP クライアントに対して設定されていて、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いないが、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、次のように受信者のタイプに基づいてそれぞれの受信者ごと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 サーバにある場合には、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 サーバにある場合には、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 Administration で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）] ページに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格納するか、ユーザの代行 SMTP アドレスにメッセージをリレーするか、または、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、リモートの 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、そのユーザのホーム サーバにメッセージをリレーします。その後、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）] ページに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、または、NDR を送信者に送信します。どちらを実行するかは、Connection の管理 の [システム設定（System Settings）] > [全般設定（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）] の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、メッセージは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）に格納します。

メッセージにセキュア 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、常にセキュア 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 メッセージにセキュアのマークを付けます。セキュア メッセージの受信、およびセキュア 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、『*Security Guide for Cisco Unity Connection*』（*Release 8.x*）の「Securing User Messages in Cisco Unity Connection 8.x」の章にある「How Cisco Unity Connection 8.x Handles Messages That Are Marked Private or Secure」の項を参照してください。（このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/unity/8x/security/guide/8xcusecx.html から入手できます）。

IMAP と Cisco Unity Connection ViewMail for Microsoft Outlook 8.x の使用例

ExampleCo の従業員は、電子メールを利用するために Microsoft Outlook を使用して Microsoft Exchange サーバにアクセスしています。この企業の各従業員は、firstname.lastname@example.com というパターンのアドレスで社内電子メールを受信します。ExampleCo では、従業員が Outlook を使用して Cisco Unity Connection サーバに保管されたボイス メッセージにアクセスできるようにしようとしています。従業員が Outlook クライアントでボイス メッセージを送信、転送、またはリレーできるように、ExampleCo は、Cisco Unity Connection ViewMail for Microsoft Outlook プラグインを導入します。各従業員の Outlook クライアントを、IMAP を使用して Connection ユーザ アカウントにアクセスするように設定します。

ExampleCo の Robin Smith が、同僚の Chris Jones に電子メールを送信するために、chris.jones@example.com 宛の新規電子メール メッセージを作成します。デフォルトでは、新規電子メール メッセージの送信は、Microsoft Exchange サーバを経由するように Outlook は設定されています。次に、Robin が Chris にボイス メッセージを送信するために、[新しいボイス メッセージ（New Voice Message）] アイコンを選択すると、ViewMail for Outlook フォームが開きます。前と同様 Robin

は、メッセージのアドレスに chris.jones@example.com を指定し、音声メッセージを録音し、[送信（Send）] ボタンを選択します。この場合、ViewMail は Connection IMAP アカウントを使用してメッセージを送信するように設定されているため、ボイス メッセージの送信は Connection サーバを経由します。

Connection は、ボイス メッセージを受信すると、SMTP プロキシ アドレスのリストで、robin.smith@example.com（送信者）および chris.jones@example.com（受信者）を検索します。これらのアドレスは、それぞれ Robin Smith および Chris Jones のユーザ プロファイルで、SMTP プロキシ アドレスとして定義されているため、Connection は、このメッセージを Smith から Chris Jones 宛のボイス メッセージとして送信します。

Chris が Outlook を開くと、Robin からの電子メール メッセージが、Microsoft Exchange Inbox に新規メッセージとして表示されます。一方、Robin からのボイス メッセージは、Connection アカウントの Inbox に、新規メッセージとして表示されます。Chris はこのアカウントに IMAP を介してアクセスします。いずれかのメッセージに Chris が返信する際は、Outlook クライアントが、元のメッセージの受信に Chris が使用したアカウントを自動的に使用して、その返信を送信します。

Connection は、ExampleCo で使用されている社内電子メール アドレスを、Connection ユーザ アカウントにマッピング（各ユーザに定義される SMTP プロキシ アドレスを使用）できるように設定されているため、ユーザは既存の Outlook アドレス帳を使用して、電子メールとボイス メッセージの両方にアドレスを指定できます。また、ユーザが、メッセージの作成、返信、転送の際に、どちらのアカウントを使用すべきか意識する必要はなく、すべて自動的に Outlook と ViewMail の設定によって処理されます。

Cisco Unity Connection 8.x での IMAP アクセス導入に関する推奨事項

IMAP クライアントを導入して 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、次の推奨事項を検討してください。

- ファイアウォールを使用して、Connection の 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 Administration 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。
- ユーザの社内電子メール アドレスを、ユーザの SMTP プロキシ アドレスとして設定してください。ユーザのワークステーションに Connection IMAP アカウントを設定する際、IMAP 設定には、Connection 固有の電子メール アドレスではなく、ユーザの社内電子メール アドレスを使用してください。これにより、電子メール クライアントでボイス メッセージのアドレスを指定するために余分な電子メール アドレスを扱う必要がなくなり、Connection SMTP ドメインが変更された場合に Connection 固有のアドレスの変更による影響を受けずにすみます。
- ViewMail for Outlook は、ユーザが到達可能なメッセージ受信者を、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。ユーザが到達可能な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に対する NDR をユーザが受信しないようにするには、ViewMail ユーザ用に、ユーザ サーチ スペース内のオブジェクトだけを登録した Outlook アドレス帳を、別個作成することを検討してください。

Cisco Unity Connection 8.x の 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てください。
   a. Connection サーバからのメッセージを受信するように SMTP スマート ホストを設定します。使用中の SMTP サーバ アプリケーションのマニュアル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、Connection サーバを設定します。「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」（P.20-5）を参照してください。
   c. プライベート メッセージやセキュア メッセージをリレーするかどうかを制御する設定を確認します。「メッセージ リレー設定の構成」（P.20-6）を参照してください。
2. Connection の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。『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』（*Release 8.x*）の「Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 8.x」の章にある「Message Actions in Cisco Unity Connection 8.x」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/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx.html から入手可能です。
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。『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』（*Release 8.x*）の「Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 8.x」の章にある「SMTP Proxy Addresses in Cisco Unity Connection 8.x」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/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx.html から入手可能です。

（注） 最低でも、各ユーザの社内電子メール アドレスを、そのユーザの SMTP プロキシ アドレスとして設定することを推奨します。

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与えられるサービス クラスに、ユーザを割り当てます。『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』（*Release 8.x*）の「Setting Up Features and Functionality That Are Controlled by Class of Service Settings in Cisco Unity Connection 8.x」の章にある「IMAP Client Access to Voice Messages in Cisco Unity Connection 8.x」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/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx.html から入手可能です。
5. IMAP クライアントからの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。『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』（*Release 8.x*）の「Managing Contacts in Cisco Unity Connection 8.x」の章にある「SMTP Proxy Addresses in Cisco Unity Connection 8.x」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/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx.html から入手可能です。
6. IMAP クライアントからの SMTP 接続を許可するよう、Connection サーバを設定します。「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」（P.20-6）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*：「Cisco Unity Connection Administration、Cisco PCA、および IMAP 電子メール クライアントからの Cisco Unity Connection 8.x へのアクセスの保護」（P.25-2）の説明に従って、セキュアな IMAP 接続を提供するよう、Connection サーバを設定します。
8. オプションとして、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。「SMTP メッセージ パラメータの設定」（P.20-8）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。『*User Workstation Setup Guide for Cisco Unity Connection*』（*Release 8.x*）の「Configuring an Email Account to Access Cisco Unity Connection 8.x Voice Messages」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/8x/user_setup/guide/8xcucuwsx.html から入手可能です。

Cisco Unity Connection 8.x での IMAP アクセスの設定手順

次の項を参照してください。

- 「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」（P.20-5）
- 「メッセージ リレー設定の構成」（P.20-6）
- 「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」（P.20-6）
- 「SMTP メッセージ パラメータの設定」（P.20-8）

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 サーバを設定するには

ステップ 1　Cisco Unity Connection Administration 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）] を選択します。

ステップ 2　[スマート ホスト（Smart Host）] ページの [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は、DNS が設定されている場合のみ入力します）。

ステップ 3　[保存（Save）] を選択します。

メッセージ リレー設定の構成

プライベートまたはセキュアのマークが付いたメッセージを、Cisco Unity Connection でリレーするかどうか選択できます。

メッセージ リレー設定の構成方法

ステップ 1　Cisco Unity Connection Administration で [システム設定（System Settings）] を展開し、[詳細設定（Advanced）] を展開して [メッセージング（Messaging）] を選択します。

ステップ 2　プライベートのマークが付いたメッセージを Cisco Unity Connection でリレーするには、[プライベート メッセージのリレーを許可する（Allow Relaying of Private Messages）] チェックボックスをオンにします（このチェックボックスはデフォルトでオンになっています）。Connection は、プライベート メッセージをリレーする際に、そのメッセージにプライベート フラグを設定します。

Connection でプライベート メッセージをリレーしないようにするには、このチェックボックスをオフにします。プライベートのマークが付いているためにリレーできないメッセージを受信した場合、Connection は、そのメッセージの送信者に NDR を送信します。

ステップ 3　Connection でセキュア メッセージをリレーするには、[セキュアメッセージのリレーを許可する（Allow Relaying of Secure Messages）] チェックボックスをオンにします（このチェックボックスはデフォルトでオフになっています）。Connection は、標準のメッセージとしてセキュア メッセージをリレーします。

Connection でセキュア メッセージをリレーしないようにするには、このチェックボックスをオフにします。セキュアのマークが付いているためにリレーできないメッセージを受信した場合、Connection は、そのメッセージの送信者に NDR を送信します。

ステップ 4　[保存（Save）] を選択します。

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 に対して SMTP 接続を確立できるクライアントを制御するために、多数のオプションが用意されています。アクセス リストを作成して、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。そのようにする場合、それらのクライアント（信頼されない 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、信頼されない IP アドレスを持つクライアント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、IMAP クライアントで、Connection エイリアスと Cisco PCA パスワード（Web アプリケーション パスワード）を入力して、認証を受けます。Connection Messaging Assistant で Cisco PCA パスワードを変更した場合は、必ず、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、ユーザに必ず知らせてください。両方のアプリケーションで Cisco PCA パスワードを更新しても、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、『*User Workstation Setup Guide for Cisco Unity Connection*』（*Release 8.x*）（http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_setup/guide/8xcucuwsx.html から入手可能）の「Configuring an Email Account to Access Cisco Unity Connection 8.x Voice Messages」の章にある「Troubleshooting IMAP Client Sign-In Problems in Cisco Unity Connection 8.x」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に従ってください。

- 「Cisco Unity Connection IP アドレス アクセス リストを設定する方法」（P.20-7）
- 「信頼されない IP アドレスに対するアクセスと認証を設定する方法」（P.20-7）

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

ステップ 1　Cisco Unity Connection Administration で、[システム設定（System Settings）] > [SMTP 設定（SMTP Configuration）] を展開し、[サーバ（Server）] を選択します。

ステップ 2　[SMTP サーバの設定（SMTP Server Configuration）] ページの [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）] を選択します。

ステップ 3　[IP アドレス アクセス リストの検索（Search IP Address Access List）] ページで [新規追加（Add New）] を選択して、新しい IP アドレスをリストに追加します。

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、「*（アスタリスク）」だけ入力し、すべての IP アドレスと一致させることもできます。

ステップ 5　[保存（Save）] を選択します。

ステップ 6　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、[アクセス IP アドレス（Access IP Address）] ページの [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）] ページの変更が終了したら、[保存（Save）] を選択します。

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 からステップ 7 を繰り返します。

信頼されない IP アドレスに対するアクセスと認証を設定する方法

ステップ 1　Cisco Unity Connection Administration で、[システム設定（System Settings）] > [SMTP 設定（SMTP Configuration）] を展開し、[サーバ（Server）] を選択します。

ステップ 2　特定の IP アドレスからの接続だけを許可するように Connection が設定されているかどうかにかかわらず、すべてのクライアントからの SMTP 接続を許可するには、[SMTP サーバの設定（SMTP Server Configuration）] ページの [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て、このようなタイプのクライアントに対して認証を行うように設定します。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いるが、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 サーバとの 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 アドレスに対して認証を要求し、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）] のどちらかに設定することを推奨します。

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。「Cisco Unity Connection Administration、Cisco PCA、および IMAP 電子メール クライアントからの Cisco Unity Connection 8.x へのアクセスの保護」（P.25-2）を参照してください。

SMTP メッセージ パラメータの設定

Connection では、設定した合計サイズよりも大きい着信 SMTP メッセージ、または設定した受信者数よりも多くの受信者を指定している、着信 SMTP メッセージを拒否することができます。デフォルトでは、Connection は 10MB よりも大きいメッセージ、または指定している受信者数が 15,000 人よりも多いメッセージを受け入れます。

SMTP メッセージ パラメータを設定する方法

ステップ 1　Cisco Unity Connection Administration で、[システム設定（System Settings）] > [SMTP 設定（SMTP Configuration）] を展開し、[サーバ（Server）] を選択します。

ステップ 2　[SMTP サーバの設定（SMTP Server Configuration）] ページの [メッセージ サイズの制限（Limit Size of Message）] フィールドに、SMTP クライアントから送信される各メッセージ サイズの制限値を、キロバイト単位で入力します。

ステップ 3　[メッセージあたりの受信者数の制限（Limit Number of Recipients per Message）] フィールドに、1 メッセージあたりの最大受信者数を入力します。

ステップ 4　[保存（Save）] を選択します。