



ユーザメッセージの保護

- [ユーザメッセージの保護 \(1 ページ\)](#)

ユーザメッセージの保護

はじめに

ユーザは、メッセージの機密性を設定することで、ボイスメッセージにアクセスできる人や、そのボイスメッセージを他の人に再配信できるかどうかを制御できます。Cisco Unity Connection には、ユーザがボイスメッセージを WAV ファイルとしてハードドライブ、または Unity Connection サーバ外の他の場所に保存することを防止する機能もあります。この機能を使用すると、メッセージをアーカイブまたは消去するまでそれらのメッセージを保持する期間を制御できます。Unity Connection はまた、メッセージのセキュアな削除を管理するためのメソッドを提供します。

プライベートまたはセキュアとマークされたメッセージの処理

ユーザが電話を使用して Cisco Unity Connection でメッセージを送信するときには、そのメッセージをプライベート、セキュア、またはその両方としてマークできます。また、外部の発信者が残したメッセージを Unity Connection でプライベート、セキュア、またはその両方としてマークするかどうかも指定できます。

プライベートメッセージ

- プライベートメッセージに IMAP クライアントからアクセスする場合、別途指定しない限り、プライベートメッセージを WAV ファイルとして転送したりローカルの場所に保存したりできます。(ユーザがプライベートメッセージを再生および転送できないようにする方法や、プライベートメッセージを WAV ファイルとして保存できないようにする方法については、「[IMAP クライアントアクセス用メッセージセキュリティオプション](#)」を参照してください)。
- ユーザがプライベートメッセージに返信するときには、プライベートとしてマークされません。

- ユーザがメッセージを送信するときに、そのメッセージをプライベートとしてマークするかどうかを選択できます。
- システムにプライベートメッセージ用のメッセージ配信と機密性オプションが設定されている場合は、外部の発信者がメッセージを残すときに、そのメッセージをプライベートとしてマークできません。
- ユーザが他のユーザにメッセージを残す前に、そのユーザのメールボックスに明示的にサインインしない場合は、メッセージをプライベートとしてマークできます（システムにこのオプションが設定されている場合）。
- デフォルトの Unity Connection では、SMTP リレー アドレスにメッセージをリレーするように1つ以上のメッセージ操作が設定されているユーザに対して、プライベートメッセージ（プライベートフラグの付いた通常のメッセージ）をリレーします。プライベートメッセージのリレーを無効にするには、Cisco Unity Connection Administration の [システム設定 (System Settings)] > [詳細設定 (Advanced)] > [メッセージング (Messaging)] ページの [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フにします。

セキュアメッセージ

- セキュアメッセージは Unity Connection サーバにだけ保存されるため、アーカイブまたは完全に削除されるまで保持される期間を制御できます。セキュアメッセージの場合、Cisco Unity Connection ViewMail for Microsoft Outlook と Cisco Unity Connection ViewMail for IBM Lotus Notes の Media Player で、[名前を付けて保存 (Save Recording As)] オプションが自動的に無効になります。
- セキュアメッセージは、メッセージ保持ポリシーを強制的に適用するのに便利です。ユーザがそのセキュアメッセージを再生したか、その他の方法で処理したかどうかに関係なく、指定した日数を超えたセキュアメッセージを自動的に削除するように、Unity Connection を設定できます。
- セキュアメッセージは、次のインターフェイスを使用して再生できます。
 - Unity Connection 電話インターフェイス
 - Web Inbox
 - Cisco ViewMail for Microsoft Outlook (バージョン 8.5 以降)
 - Cisco Unity Connection ViewMail for IBM Lotus Notes
 - Cisco Unified Mobile Communicator および Cisco Mobile
 - Cisco Unified Messaging with IBM Lotus Sametime バージョン 7.1.1 以降 (Cisco Unified Messaging with Lotus Sametime を使用したセキュアメッセージの再生に関する要件については、該当する『Release Notes for Cisco Unified Messaging with IBM Lotus Sametime』(http://www.cisco.com/c/en_US/support/unified_communications/unified_communications_messaging_callmgr/products/release-notes.html) を参照してください。)
- セキュアメッセージは、次のインターフェイスを使用して転送できます。

- Unity Connection 電話インターフェイス
 - Web Inbox
 - Cisco Unity Connection ViewMail for Microsoft Outlook 8.5
- 次のインターフェイスを使用してセキュアメッセージにアクセスすることはできません。
- IMAP クライアント（ViewMail for Outlook または ViewMail for Notes がインストールされている場合を除く）
 - RSS リーダー
- デフォルトでは、ローカル ネットワーキング サイトをホームとしている Unity Connection ユーザだけが、セキュア メッセージを受信できます。リモート ネットワーキング サイトをホームとしている VPIM 連絡先またはユーザもメッセージを受信できますが、受信するためには、セキュアメッセージの配信を許可するように VPIM ロケーションまたはサイト間リンクが設定されている必要があります。メッセージが Unity Connection サイトを離れるか、VPIM ロケーションに送信されると、メッセージのセキュリティを保証できません。
- セキュア メッセージへの応答も、セキュアとしてマークされます。
- セキュア メッセージは、他の Unity Connection ユーザ、および同報リストにある Unity Connection ユーザに転送できます。転送されたメッセージもまた、セキュアとしてマークされます。ユーザは、転送されたメッセージおよび応答の機密性を変更できません。
- ユーザが Unity Connection にサインインしてメッセージを送信するとき、サービスクラス設定によって、メッセージをセキュアとしてマークするかどうかが決まります。デフォルトでは、ユーザがメッセージをプライベートとしてマークすると、Unity Connection でそのメッセージが自動的にセキュアとしてマークされます。
- Unity Connection がユーザにメッセージがセキュアとしてマークされたことをアナウンスするよう設定するには、[システム設定 (System Settings)] > [詳細設定 (Advanced Settings)] > [カンパセーションの設定 (Conversation Configuration)] ページで、[メッセージヘッダーでセキュアステータスをアナウンスする (Announce Secure Status in Message Header)] 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をオンにすると、Unity Connection はセキュアメッセージを再生する前に、このメッセージが「...secure message...」であることをユーザに通知するプロンプトを再生します。
- 発信者がユーザまたはコールハンドラのグリーティングに転送され、メッセージを残した場合、ユーザまたはコールハンドラ アカウントの [編集 (Edit)] > [メッセージ設定 (Message Settings)] ページの [セキュアにする (Mark Secure)] チェックボックスの状態によって、Unity Connection でメッセージがセキュアとしてマークされるかどうかが決まります。
- デフォルトでは、SMTP リレーアドレスにメッセージをリレーする 1 つ以上のメッセージ操作が設定されたユーザに対して、Unity Connection でセキュアメッセージがリレーされません。リレーが設定されたユーザに対するセキュアメッセージを受信すると、Unity Connection は、メッセージの送信者に不達確認を送信します。セキュアメッセージを Unity Connection でリレーするように設定するには、Cisco Unity Connection Administration の [シ

システム設定 (System Settings)]>[詳細設定 (Advanced)]>[メッセージング (Messaging)] ページの [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をオンにすると、セキュアメッセージはセキュア フラグ付きでリレーされますが、ほとんどの電子メールクライアントでは通常のメッセージとして扱われます。

- ファクス サーバから送られるファクス メッセージは、セキュアとしてマークされることはありません。

セキュア メッセージに関する ViewMail の制限事項

- セキュア メッセージは Cisco Unity Connection ViewMail for Microsoft Outlook 8.0 または ViewMail for IBM Lotus Notes を使用して転送することはできません。
- ViewMail for Outlook 8.0 と ViewMail for Notes ではセキュア メッセージの再生だけがサポートされています。
- ViewMail for Outlook 8.0 または ViewMail for Notes を使用して作成または応答されたメッセージは、[セキュアメッセージング (Require Secure Messaging)] フィールドが [常時 (Always)] または [選択可能 (Ask)] に設定されているサービスクラスにユーザが割り当てられている場合でも、セキュアとして送信されることはありません。

すべてのメッセージをセキュアとしてマークするための Unity Connection の設定

すべてのメッセージをセキュアとしてマークするには、次のタスク リストを使用して Unity Connection を設定します。

1. メッセージが常にセキュアとしてマークされるように、すべてのサービスクラスを設定します。「[サービスクラス \(COS\) メンバーのメッセージセキュリティの有効化](#)」を参照してください。(ユーザが Unity Connection にサインインしてメッセージを送信するとき、サービスクラス設定によって、メッセージをセキュアとしてマークするかどうかが決まります。)
2. すべての外部発信者のメッセージがセキュアとしてマークされるように、ユーザ メールボックスを設定します。「[外部の発信者が残したメッセージをセキュアとしてマークするようにユーザおよびユーザ テンプレートを設定する](#)」を参照してください。
3. すべての外部発信者のメッセージがセキュアとしてマークされるように、コールハンドラを設定します。「[外部の発信者が残したメッセージをセキュアとしてマークするようにユーザおよびユーザ テンプレートを設定する](#)」を参照してください。
4. Unity Connection がユーザにメッセージがセキュアとしてマークされたことをアナウンスしないようにするには、[システム設定 (System Settings)]>[詳細設定 (Advanced Settings)]>[カンバセーションの設定 (Conversation Configuration)] ページで、[メッセージヘッダーでセキュアステータスをアナウンスする (Announce Secure Status in Message Header)] チェックボックスをオフにします。

サービスクラス (COS) メンバーのメッセージセキュリティの有効化

- ステップ 1** Cisco Unity Connection Administration で、変更または新規作成する COS を探します。
- ステップ 2** [サービスクラスの編集 (Edit Class of Service)] ページで、[メッセージオプション (Message Options)] の下の [セキュアメッセージングを必須にする (Require Secure Messaging)] リストから [常時 (Always)] を選択します。
- ステップ 3** [保存 (Save)] を選択します。
- ステップ 4** 各サービスクラスに対して **ステップ 1** ~ **ステップ 3** を繰り返します。または、[一括編集 (Bulk Edit)] オプションを使用して、複数のサービスクラスを一度に編集することもできます。

外部の発信者が残したメッセージをセキュアとしてマークするようにユーザおよびユーザテンプレートを設定する

- ステップ 1** Cisco Unity Connection Administration で、編集するユーザアカウントまたはテンプレートを探します。
複数のユーザを同時に編集するには、[ユーザの検索 (Search Users)] ページで該当するユーザのチェックボックスをオンにしてから、[一括編集 (Bulk Edit)] を選択します。
- ステップ 2** [編集 (Edit)] メニューで、[メッセージ設定 (Message Settings)] を選択します。
- ステップ 3** [メッセージ設定の編集 (Edit Message Settings)] ページで、[メッセージセキュリティ (Message Security)] の下の [セキュアにする (Mark Secure)] オプションを選択します。
一括編集モードで編集する場合は、最初に [セキュアにする (Mark Secure)] フィールドの左側にあるチェックボックスをオンにして、選択されたユーザまたはテンプレートのフィールドが変更されることを示す必要があります。
- ステップ 4** [保存 (Save)] を選択します。

外部の発信者が残したメッセージをセキュアとしてマークするようにコールハンドラおよびコールハンドラテンプレートを設定する

- ステップ 1** Cisco Unity Connection で、編集するコールハンドラまたはコールハンドラテンプレートを探します。
複数のコールハンドラを同時に編集するには、[コールハンドラの検索 (Search Call Handlers)] ページで該当するコールハンドラのチェックボックスをオンにしてから、[一括編集 (Bulk Edit)] を選択します。
- ステップ 2** [編集 (Edit)] メニューで、[メッセージ設定 (Message Settings)] を選択します。
- ステップ 3** [メッセージ設定の編集 (Edit Message Settings)] ページで、[メッセージセキュリティ (Message Security)] の下の [セキュアにする (Mark Secure)] チェックボックスをオンにします。
一括編集モードで編集する場合は、最初に [セキュアにする (Mark Secure)] フィールドの左側にあるチェックボックスをオンにして、選択されたユーザのフィールドが変更されることを示す必要があります。
- ステップ 4** [保存 (Save)] を選択します。

セキュアな削除のためのメッセージ ファイルの破棄

ユーザによる単純なメッセージの削除に加えて、組織によっては、メッセージの削除にセキュリティの追加が必要な場合があります。この場合、Cisco Unity Connection Administration の [詳細設定 (Advanced Settings)] > [メッセージングの設定 (Messaging Configuration)] ページで、[メッセージファイルの破棄レベル (Message File Shredding Level)] の設定を行います。これはシステム全体の設定であり、メッセージの削除時に指定された回数の破棄が行われ、ユーザによって削除されたメッセージのコピーがセキュアに削除されます。この機能を有効にするには、0 (ゼロ) 以外の値を入力します。フィールドに入力する設定値 (1 ~ 10 までの数字) は、削除されたメッセージファイルが破棄される回数を示します。破棄は、Linux 標準の破棄ツールを介して行われます。メッセージを構成する実際のビットが、ランダムなデータのビットによって指定された回数上書きされます。

デフォルトでは、[削除済みメッセージの消去 (Clean Deleted Messages)] sysagent タスクが実行されるたびに、破棄プロセスが 30 分ごとに発生します。[削除済みメッセージの消去 (Clean Deleted Messages)] は、読み取り専用タスクです。このタスクの設定値は変更できません。

(タスクに関する情報は Cisco Unity Connection Administration の [ツール (Tools)] > [タスク管理 (Task Management)] で参照できます)。

メッセージのコピーまたはメッセージに関連するファイルが破棄されない場合もあります。

- 通常メッセージ送信プロセスでは、一時オーディオファイルが作成されます。これらの一時オーディオファイルは、メッセージ送信時に削除されますが、破棄はされません。メッセージへの参照は削除されますが、オペレーティングシステムにスペースを再利用する理由が生じてデータが上書きされるまで、実際のデータは、ハードドライブ上に維持されます。これらの一時オーディオファイルに加えて、削除され破棄されたメッセージを配信する場合に使用される他の一時ファイルもあります (破棄をイネーブルにしている場合)。一時ファイルは、関連付けられているメッセージが削除されるとただちに破棄されることに注意してください。メッセージ自体とは異なり、一時ファイルは [削除済みメッセージの消去 (Clean Deleted Messages)] sysagent タスクの実行を待機しません。
- ユーザが Web Inbox で再生不能なファイル形式のメッセージを再生しようとした場合、メッセージは一時オーディオファイルにトランスコードされます。この一時オーディオファイルは、ユーザがメッセージを削除すると同時に削除されますが、破棄はされません。
- 破棄は、Unity Connection サーバ上に存在するメッセージにだけ発生する場合があります。メッセージが他のサーバから回復できないことを保障するには、次の機能を使用しないでください：メッセージリレー、IMAP、ViewMail for Outlook、ViewMail for Notes、Web Inbox、単一受信トレイ、SameTime Lotus プラグイン、Cisco Unified Personal Communicator、Cisco Mobile、またはネットワーク接続されたサーバ間の SMTP スマート ホスト。これらの機能を使用する場合は、セキュアなメッセージング機能を使用する必要があります。セキュアメッセージングを使用する場合、セキュアメッセージのローカルコピーは作成されず、ユーザもローカルコピーの保存を許可されないため、メッセージのすべてのコピーが Unity Connection サーバ上に残り、削除時に破棄されます。



注 セキュア メッセージングに関する追加情報については、「[プライベートまたはセキュアとマークされたメッセージの処理](#)」を参照してください。

- **Unity Connection** ネットワーク内のロケーション間で送信されるメッセージは、送信前に一時的なロケーションに書き込まれます。このメッセージの一時コピーは削除されますが、破棄されません。

Unity Connection クラスタで破棄をイネーブルにした場合、メッセージはプライマリ サーバとセカンダリサーバの両方で削除時に破棄されます。

パフォーマンスの問題により、破棄レベルを3よりも高く設定しないことを強く推奨します。メッセージは完全削除された場合にだけ破棄されることに注意してください。

IMAP クライアント アクセス用メッセージセキュリティ オプション

機密性が通常またはプライベートとしてマークされているボイスメッセージにユーザがIMAPクライアントからアクセスするときに、IMAP クライアントで、ユーザがメッセージを WAV ファイルとしてハードディスクに保存したり、メッセージを転送したりするのが許可されることがあります。ユーザがIMAPクライアントを使用してボイスメッセージを保存または転送するのを防止する場合は、次のサービス クラス オプションのいずれかを指定することを検討してください。

- ユーザは、メッセージの機密性に関係なく、IMAP クライアントでメッセージヘッダーにだけアクセスできる。
- ユーザは、プライベートとしてマークされているメッセージを除くすべてのメッセージのメッセージ本文にアクセスできる。（クライアントが Microsoft Outlook で ViewMail for Outlook がインストールされている場合、またはクライアントが Lotus Notes で ViewMail for Notes がインストールされている場合を除き、IMAP クライアントではセキュアメッセージにアクセスできません）。

