Cisco Unity Connection でのユーザ メッセージの保護

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。

次の項を参照してください。

- 「Cisco Unity Connection で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方法」（P.11-1）
- 「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 Cisco Unity Connection の設定」（P.11-4）
- 「Cisco Unity Connection での 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」（P.11-6）

Cisco Unity Connection で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方法

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、「Cisco Unity Connection での 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」（P.11-6）を参照してください)。
- ユーザがプライベート メッセージに応答するときには、プライベートとしてマークされます。

- 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）。
- デフォルトでは、Unity Connection 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 の管理 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 メッセージについては、Cisco Unity Connection ViewMail for Microsoft Outlook（バージョン 8.0）、および Cisco Unity Connection ViewMail for IBM Lotus Notes の Media Master の [オプション（Options）] メニューで、[名前を付けて保存（Save Recording As）] オプションが自動的にディセーブルになります。
- 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 Cisco Unity Connection Web Inbox（Unity Connection10.x）Cisco Unity Connection ViewMail for Microsoft Outlook （バージョン 8.0）
  - Cisco ViewMail for Microsoft Outlook（バージョン 8.5 以降）
  - Cisco Unity Connection ViewMail for IBM Lotus Notes
  - Cisco Unified Personal Communicator バージョン 7.0 以降
  - 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 を使用してセキュア メッセージを再生する際の要件については、該当する『*Release Notes for Cisco Unified Messaging with IBM Lotus Sametime*』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/ps9830/prod_release_notes_list.html から入手可能です）。
- 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転送できます。
  - Unity Connection 電話インターフェイス
  - Cisco Unity Connection Unity Connection Web Inbox（Unity Connection 10.x）
  - 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。
- *（Cisco Unity Connection 10.x）*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 の管理 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 [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 を使用して転送できません。
- ViewMail for Outlook 8.0 および ViewMail for Notes は、セキュア メッセージの再生だけをサポートします。
- 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 [選択する（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 Cisco 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 Cisco 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。「COS メンバーのメッセージ セキュリティをイネーブルにするには」（P.11-4）の手順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には」（P.11-4）の手順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には」（P.11-5）の手順を参照してください。
4. *（Cisco Unity Connection 10.x）*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設定するには、[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。

COS メンバーのメッセージ セキュリティをイネーブルにするには

ステップ 1　Cisco Unity Connection の管理 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（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 からステップ 3 までを繰り返します。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には

ステップ 1　Cisco Unity Connection の管理 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には

ステップ 1　Cisco Unity Connection の管理 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 の管理 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ときに、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 [ツール（Tools）] > [タスク管理（Task Management）] の下の [Cisco Unity Connection の管理（Cisco Unity Connection の管理）] 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。

- 通常の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 ファイルに変換されます。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収されないようにするには、メッセージ リレー、IMAP、ViewMail for Outlook、ViewMail for Notes、Web Inbox または Cisco Unified Personal Communicator、単一受信トレイ、SameTime Lotus プラグイン、Cisco Mobile、またはネットワーク サーバ間の SMTP スマート ホストで次の機能を使用しないでください。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。セキュアなメッセージングを使用する場合、セキュアな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） セキュアなメッセージングに関する追加情報については、「セキュア メッセージ」（P.11-2）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。

Cisco 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。

Cisco Unity Connection での 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）。