CHAPTER 16

安全なプライベート メッセージ機能の設定

Cisco Unity Connection では、プライベートのマークが付いたメッセージは、電話または Cisco Unity Inbox から転送できません。どのユーザも、自分が送信するメッセージにプライベートのマークを付けることができます。また、メッセージにプライベートのマークが付いている場合、Cisco Unity Inbox の Media Master のオプション メニューにある［名前を付けて保存］オプションは無効になります。

さらに強力なセキュリティを必要とするユーザがいる場合は、安全なメッセージ機能を設定して、ユーザが使用できるようにすることを検討してください。安全なメッセージ機能では、ユーザが電話で Connection にログオンして録音するボイス メッセージに対する公開鍵 / 秘密鍵暗号化により、セキュリティが提供されます。安全のマークを付けることによって暗号化されたボイス メッセージは、Connection サーバをホームとする Connection ユーザ以外は聞くことができません。

暗号化された安全なメッセージの送信が有効になっているユーザがメッセージを送信するときは、Connection ガイダンスで「プライバシーの保障されたメッセージとして設定するには、3 を押してください」と再生されます。このメッセージは、暗号化され、プライベートのマークが付けられて、転送することができなくなります。暗号化された安全なメッセージの送信が有効になっていないユーザには、「プライベートに設定するには 3...」と再生され、ユーザが 3 を押すとこのメッセージは転送できなくなります。ユーザは、Cisco Personal Communications Assistant からもメッセージに安全とプライベートのマークを付けることができます。

セキュリティ強化策として、ボイス メッセージの機密性に関係なく、ボイス メッセージをユーザがハードディスクに保存できないように設定することもできます。これを行うには、Cisco Unity Inbox の Media Master のオプション メニューにある［名前を付けて保存］オプションを使用不可にします。

この章は、次の項で構成されています。

安全なメッセージ機能の概要

安全なメッセージ機能では、ボイス メッセージに対する公開鍵 / 秘密鍵暗号化により、セキュリティが提供されます。ユーザがボイス メッセージを録音して安全のマークを付けると、Cisco Unity Connection は Connection サーバの公開鍵を使用して WAV ファイルを暗号化します。Connection サーバの公開鍵は、Connection データベースに格納されています。安全なメッセージを送信するには、ユーザは Connection に電話でログオンします。または、電話またはメディア再生ソフトウェアを使用してメッセージを録音し、Cisco Unity Inbox から送信します。安全なメッセージは、他のボイス メッセージと同様に、組織内外の任意の電話を使用して録音することができます。

安全なメッセージを再生するために、Connection はサーバに格納されている秘密鍵を使用してメッセージを暗号解除します。Connection が安全なメッセージを再生できるのは、受信者が発信者と同じ Connection サーバをホームにしている場合のみです。メッセージを聞くには、受信者は Connection に電話でログオンします。または、Cisco Unity Inbox を使用して、電話またはメディア再生ソフトウェアを使用してメッセージを聞きます。受信者は、組織内外の任意の電話を使用してメッセージを聞くことができます。Connection サーバ以外のサーバに関連付けられている受信者は、必要な秘密鍵を入手できないため、安全なメッセージを聞くことはできません。代わりに、Connection によって次のような案内用の WAV ファイルが再生されます。

> 「このボイスメッセージは、プライバシーの保障されたメッセージで、電話から ボイスメールシステムにログオンし、メッセージを確認するときにのみ再生できるようになっています。もし間違って、このメッセージを受け取った場合は、送信者に通知を行い、直ちに削除してください。」

Connection は、安全なメッセージをユーザがメディア再生ソフトウェアを使用して再生しようとすると、この案内メッセージを再生します。また、ユーザが電話を Media Master の再生デバイスとして指定している場合でも、安全なメッセージをユーザが Cisco Unity Inbox を使用して再生しようとすると、この案内メッセージが再生されます。

他にも、受信者が安全なメッセージを SMTP 電子メール プログラムを使用して再生しようとすると、次のテキスト メッセージが表示されます。

> 「This message and any files transmitted with it are confidential and intended solely for the individual or entity to which they are addressed.If you received this message in error, notify the sender and delete it immediately.」

（注） ユーザは、ユーザ　スピーチ認識ガイダンスまたは任意のキー入力バージョンを使用して、安全なメッセージを送受信することができます。

安全なメッセージ機能の制限事項

安全なメッセージ機能には、次の制限事項があることを考慮してください。ユーザ、管理者、およびサポート デスク担当者がこの制限事項を把握していることを確認してください。

- ユーザが別のユーザに電話をかけて、ボイスメールに転送された後にボイス メッセージを残すときは、メッセージにプライベートまたは安全のマークを付けることができません。
- 安全なメッセージの暗号解除に必要な秘密鍵は、個々のユーザまたはワークステーションに固有のものもではありません。このため、発信者が宛先指定を間違えたり、システムに問題が発生したりしたために、安全なメッセージが意図しない受信者に送信された場合でも、受信者が発信者と同じ Connection サーバをホームにしている限り、Connection はメッセージを受信したすべての受信者にメッセージを再生します。
- ユーザは、IMAP クライアントからは安全なメッセージを送信できず、取得することもできません。ユーザが安全なメッセージを聞こうとすると、代わりに案内メッセージが再生され、メッセージを聞くには Connection に電話でログオンする必要があると通知されます。

- [System Settings] > [Advanced] > [Secure Messaging] ページの [Encrypt All Messages from Outside Callers] 設定と [Encrypt All Private Messages from Users] 設定を有効にすると、ユーザはどのメッセージも IMAP クライアントを使用して聞くことができなくなります。代わりに、Connection ガイダンスまたは Cisco Unity Inbox からメッセージを聞く必要があります。

安全なメッセージ機能の設定

インストール中に、安全なメッセージ機能のための証明書が Cisco Unity Connection サーバに自動的にインストールされます。また、管理者が設定するエージング ポリシーとタスク スケジュールに従って、証明書を作成または削除するタスクを自動的に実行するように Connection が設定されます。

次のタスク リストを使用して、安全なメッセージ機能を設定します。

1. 証明書のエージング ポリシーを設定します。P.16-3 の 手順「安全なメッセージ機能の証明書にエージング ポリシーを設定する」を参照してください。

   証明書の作成と削除は、8:1 の比率で実行することをお勧めします。たとえば、[Weeks Before Deleting Old Certificate] を 16 週に設定する場合は、[Weeks Before Creating New Certificate] を 2 週に設定します。この例では、新しい証明書が 2 週ごとに作成され、証明書は存在期間が 16 週に達すると削除されます。

   安全なメッセージをユーザが保存した場合、ユーザがメッセージを聞くことのできる期間は、メッセージに関連付けられている証明書が Connection サーバ上に存在する間のみであることに注意してください。比率を 8:1 に設定しておくと、既存の証明書がシステムから必要以上に早く削除されることがなくなります。

   新しい証明書は、既存の証明書を削除しない場合は定期的に作成しないようにしてください。既存の証明書を削除しないまま、サーバ上に新しい証明書を複数作成すると、パフォーマンスに悪影響を及ぼす可能性があります。

2. 必要な場合は、Certificate Management タスクに関連付けられているデフォルトのタスク スケジュールを調整します。P.16-4 の 手順「安全なメッセージ機能の証明書を自動作成および自動削除するタスク スケジュールを修正する」を参照してください。このタスクは、デフォルトのスケジュールに従って実行することをお勧めします。

3. ユーザの安全なメッセージ機能を有効にします。次のような方法があります。
   - すべてのユーザの安全なメッセージ機能を有効にする。P.16-5 の 手順「安全なメッセージ機能をシステム全体で有効にする」を参照してください。
   - 個々のユーザの安全なメッセージ機能を有効にする。P.16-6 の 手順「個々のユーザの安全なメッセージ機能を有効にする」を参照してください。
   - ユーザ テンプレートを使用して、特定のユーザ グループの安全なメッセージ機能を有効にする。P.16-6 の 手順「ユーザ テンプレートを使用して複数のユーザの安全なメッセージ機能を有効にする」を参照してください。たとえば、営業部のすべての従業員が安全なメッセージ機能を使用できるようにするには、Sales Department ユーザ テンプレートを設定して、このテンプレートに対して機能を有効にし、営業部員のアカウントを設定するときにこのテンプレートを使用します。ユーザ テンプレートに対してこの機能を有効にしても、そのテンプレートに基づいて作成された既存のユーザ アカウントには影響しないことに注意してください。安全なメッセージ機能が有効になるのは、テンプレートに対して機能を有効にした後に、そのテンプレートに基づいて作成されるユーザのアカウントのみです。

安全なメッセージ機能の証明書にエージング ポリシーを設定する

ステップ 1　Cisco Unity Connection Administration で、**[System Settings] > [Advanced]** を展開し、**[Secure Messaging]** をクリックします。

ステップ 2　[Secure Messaging Configuration] ページで、次のフィールドに値を入力します。

- [Weeks Before Creating New Certificate]：0 ～ 52 週の値を入力します。値を 0 にした場合、新しい証明書は一切作成されません。
- [Weeks Before Deleting Old Certificate]：0 ～ 52 週の値を入力します。値を 0 にした場合、既存の証明書は一切削除されません。

（注）　証明書の作成と削除は、8:1 の比率で実行することをお勧めします。たとえば、[Weeks Before Deleting Old Certificate] を 16 週に設定する場合は、[Weeks Before Creating New Certificate] を 2 週に設定します。この例では、新しい証明書が 2 週ごとに作成され、証明書は存在期間が 16 週に達すると削除されます。

ステップ 3　**[Save]** をクリックします。

安全なメッセージ機能の証明書を自動作成および自動削除するタスク スケジュールを修正する

ステップ 1　Cisco Unity Connection Administration で、**[Tools]** を展開し、**[Task Management]** をクリックします。

ステップ 2　[Task Definitions] ページで、テーブルの **[Certificate Management]** をクリックします。

ステップ 3　[Task Definition Basics] ページで、[Edit] メニューの **[Task Schedule]** をクリックします。

ステップ 4　[Task Schedule] ページで、デフォルトのスケジュールを必要に応じて調整し、証明書の自動作成と自動削除を制御します。

デフォルト設定に戻す場合は、**[Set to Defaults]** をクリックします。

注意　Certificate Management タスクが実行されると、前の「安全なメッセージ機能の証明書にエージング ポリシーを設定する」の手順で設定したエージング ポリシーの値がまず確認され、条件に該当する場合のみ証明書が作成または削除されます。このタスクは、月に 1 回のみ実行するように設定しないでください。このように設定すると、予期しない結果が生じる恐れがあります。このタスクは、デフォルトのスケジュールに従って実行することをお勧めします。

ステップ 5　**[Save]** をクリックします。

ユーザの安全なメッセージ機能の有効化

ユーザが Cisco Unity Connection ガイダンスを使用して安全なメッセージを送信できるようにするには、ユーザの安全なメッセージ機能を有効にする必要があります。すべてのユーザに対して、システム全体で安全なメッセージ機能を有効にすることも、一部のユーザに対して有効にすることもできます。

特定のユーザに対してのみ安全なメッセージ機能を有効にすると、この機能をすべてのユーザに対してシステム全体で有効にする場合よりも、システム管理、トラブルシューティング、およびトレーニングが労働集約的になります。たとえば、安全なメッセージを受信するユーザは、安全なメッセージの送信が有効になっていないにもかかわらず、安全なメッセージを送信しようとすることがあります。このユーザは、Connection が正常に動作していないと考える可能性があります。

ユーザは、安全なメッセージの受信と再生については自動的に許可されます。一方、ユーザが安全なメッセージを送信するには、管理者が個別に有効にする必要があります。

ユーザのニーズに応じて、次のいずれかの方法を選択します。

- 安全なメッセージ機能をシステム全体で有効にする（P.16-5）
- 個々のユーザの安全なメッセージ機能を有効にする（P.16-6）
- ユーザ テンプレートを使用して複数のユーザの安全なメッセージ機能を有効にする（P.16-6）

（注） ユーザ テンプレートの追加または修正については、『*Cisco Unity Connection ユーザの移動、追加、変更 ガイド*』の「ユーザ テンプレートの追加、修正、削除」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/products/ps6509/prod_maintenance_guides_list.html から入手可能です。

安全なメッセージ機能をシステム全体で有効にする

ステップ 1　Cisco Unity Connection Administration で、**[System Settings] > [Advanced]** を展開し、**[Secure Messaging]** をクリックします。

ステップ 2　[Secure Messaging Configuration] ページで、必要に応じて次のチェックボックスをオンにします。

- [Encrypt All Messages from Outside Callers]：このチェックボックスをオンにすると、外部発信者が残すすべてのメッセージが、暗号化された安全なメッセージになります。
- [Encrypt All Private Messages from Users]：このチェックボックスをオンにすると、ユーザがメッセージにプライベートと安全のマークを付けた場合（Connection ガイダンスの送信オプション メニュー「プライバシーの保障されたメッセージとして設定するには、3 を押してください」を使用）、そのメッセージは暗号化された安全なプライベート メッセージになります。
- [Encrypt All Messages from Users]：このチェックボックスをオンにすると、メッセージ送信時に暗号化オプションを選択していない場合でも、ユーザが送信するすべてのメッセージが暗号化された安全なメッセージになります。

ステップ 3　**[Save]** をクリックします。

個々のユーザの安全なメッセージ機能を有効にする

ステップ 1　Cisco Unity Connection Administration で、**[System Settings] > [Advanced]** を展開し、**[Secure Messaging]** をクリックします。

ステップ 2　[Secure Messaging Configuration] ページで、**[Encrypt All Private Messages from Users]** チェックボックスと **[Encrypt All Messages from Users]** チェックボックスがオフになっていることを確認します。

ステップ 3　**[Users]** をクリックします。

ステップ 4　[Search Users] ページの [Search Results] テーブルで、対象となるユーザのエイリアスをクリックします。

（注）　ユーザのエイリアスが検索結果テーブルに表示されていない場合は、ページ上部の検索フィールドに必要なパラメータを設定して、**[Find]** をクリックします。

ステップ 5　[Edit User Basics] ページで、[Edit] メニューの **[Send Message Settings]** をクリックします。

ステップ 6　[Send Message Settings] ページで、**[Encrypt Private Messages]** チェックボックスをオンにします。

ステップ 7　**[Save]** をクリックします。

ステップ 8　ユーザごとにステップ 3 ～ステップ 7 を繰り返します。

ユーザ テンプレートを使用して複数のユーザの安全なメッセージ機能を有効にする

ステップ 1　Cisco Unity Connection Administration で、**[System Settings] > [Advanced]** を展開し、**[Secure Messaging]** をクリックします。

ステップ 2　[Secure Messaging Configuration] ページで、**[Encrypt All Private Messages from Users]** チェックボックスと **[Encrypt All Messages from Users]** チェックボックスがオフになっていることを確認します。

ステップ 3　Cisco Unity Connection Administration で、**[Templates]** を展開し、**[User Templates]** をクリックします。

ステップ 4　[Search User Templates] ページで、**[Add New]** をクリックします。

（注）　または、既存のテンプレートを修正することもできます。そのテンプレートに基づいて作成された既存のユーザ アカウントは、テンプレートに対してここで加える変更の影響を受けないことに注意してください。既存のテンプレートを修正する場合は、ステップ 8 に進みます。

ステップ 5　[New User Template] ページで、適切な設定を入力します。

ステップ 6　**[Save]** をクリックします。

ステップ 7　[User Templates Basics] ページで、必要に応じてその他の設定を入力します。ページ上でいずれかの設定を変更した場合は、**[Save]** をクリックします。

ステップ 8　[Edit] メニューの **[Conversation Settings]** をクリックします。

ステップ 9　[Edit Conversation Settings] ページで、**[Encrypt Private Messages]** チェックボックスをオンにします。

ステップ 10　**[Save]** をクリックします。

このテンプレートを使用して新しいユーザ アカウントを作成すると、そのユーザは安全なメッセージ機能が有効になります。

Media Master の［名前を付けて保存］オプションの無効化

デフォルトでは、プライベートのマークが付いたメッセージを除いて、ユーザは Cisco Unity Inbox の Media Master のオプション メニューにある［名前を付けて保存］オプションを使用すると、メッセージを WAV ファイルとしてハードディスクに保存できます。ボイス メッセージの機密性に関係なく、ボイス メッセージをユーザがハードディスクに保存できないように設定できます。これを行うには、Cisco Unity Inbox の Media Master のオプション メニューにある［名前を付けて保存］オプションを使用不可にします。

ただし、次のことに注意してください。

- Cisco Unity Inbox の Media Master の［名前を付けて保存］オプションを無効にした場合でも、ユーザは Cisco Personal Communications Assistant Web ツールのオプションを使用することで、グリーティングや名前の録音を保存できます。
- ユーザがメッセージをハードディスクに保存してアーカイブすることを禁止すると、ユーザは、メッセージを［受信ボックス］フォルダと［削除済みアイテム］フォルダに長い間残しておく傾向があります。
- ［名前を付けて保存］オプションを無効にすると、Connection サーバに関連付けられているすべてのユーザに影響します。特定のユーザについてのみ無効にすることはできません。

Cisco Unity Inbox の Media Master の［名前を付けて保存］オプションを無効にする

ステップ 1　Cisco Unity Connection Administration で、**[Settings] > [Advanced]** を展開し、**[PCA]** をクリックします。

ステップ 2　[PCA Configuration] ページで、**[Unity Inbox: Disable Save Recording As Option in Media Master]** チェックボックスをオンにします。

ステップ 3　**[Save]** をクリックします。