最初のセキュアメッセージを開く

この章では、パスワードで保護されたセキュアメッセージを初めて受信した際の操作手順を紹介します。Cisco Secure Email Encryption Service に登録し、セキュアメッセージを開封する方法について説明します。

この章は、次の内容で構成されています。

（注） このガイドの最新バージョンと、Cisco Secure Email Encryption Service に関するその他のドキュメントは、https://www.cisco.com/c/en/us/support/security/email-encryption/products-user-guide-list.html から入手できます。

重要 Web ブラウザで JavaScript が無効になっている場合、一部の Web ページは機能しません。

重要 Internet Explorer を使用して Web ページにアクセスする場合は、アライメントの問題が発生する可能性があります。次のサポートされているブラウザのいずれかに切り替えることをお勧めします。

- Google Chrome
- Mozilla Firefox
- Safari（MAC オペレーティングシステムの場合）

セキュアメッセージの概要

セキュアメッセージは、暗号化された電子メールメッセージの一種です。パスワードによって保護されているセキュアメッセージや、暗号化されていてもパスワードを必要としないセキュアメッセージもあります。

パスワードで保護されたセキュアメッセージを受信した場合は、Cisco Secure Message Service で無料のユーザーアカウントを設定して暗号化されたメッセージを開封する必要があります。

登録を済ませると、アカウントのパスワードを使用して受信したすべてのセキュアメッセージを開くことができます。また、このサービスを使用して、独自のセキュアメッセージを送信および管理することもできます。

セキュアメッセージを使用する理由

セキュアメッセージを使用すると、暗号化された電子メールを簡単に送受信できます。通常、メッセージの送信者は、重要な情報や機密情報を安全に相手へ伝えるためにメッセージを暗号化します。暗号化によって、予想外の機密保護違反や意図的な違法性のあるおよび悪意のある機密保護違反から大切な情報を守ります。個人または組織がセキュアメッセージを送信する場合、ほとんどはメッセージ受信者のために機密情報を保護することを目的として使用されます。また、政府の規制や法令によって、メッセージの送信者が情報の機密性を維持する必要がある場合もあります。たとえば、セキュアメッセージを使用して、医療組織が患者の病歴に関する機密情報を送信したり、金融機関が顧客の銀行口座に関する機密情報を送信したりすることもできます。

セキュアメッセージの通知

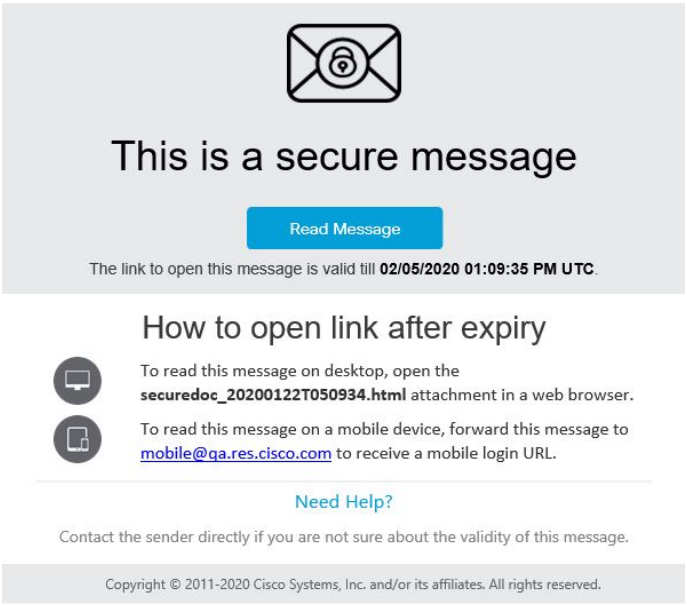
セキュアメッセージが送信されると、次のファイルを受信します。

- **通知メールメッセージ。**暗号化された安全なメッセージをセキュアメッセージの形式で受信したことを知らせます。また、セキュアメッセージおよびEncryption Serviceに関する情報へのリンクも含まれています。
- **暗号化されたメッセージの添付ファイル。**通知メッセージには、暗号化されたメッセージの添付ファイルが含まれます。この添付ファイルは、securedoc_*date*T*time*.html という命名規則を使用します。ここで、*date* と *time* はファイルに付加されたタイムスタンプです。たとえば、securedoc_20100615T193043.html というファイルを受信した場合、20100615 が年月日を表し、193043 が時刻を表します。このファイルには、セキュアメッセージと暗号化されたコンテンツの両方が含まれています。セキュアメッセージを表示するには、添付ファイルをハードドライブに保存します。次に、このファイルをダブルクリックして、セキュアメッセージをWebブラウザに表示します。通常、コンピュータでセキュアメッセージを正しく表示してメッセージを復号するには、インターネット接続が必要です。

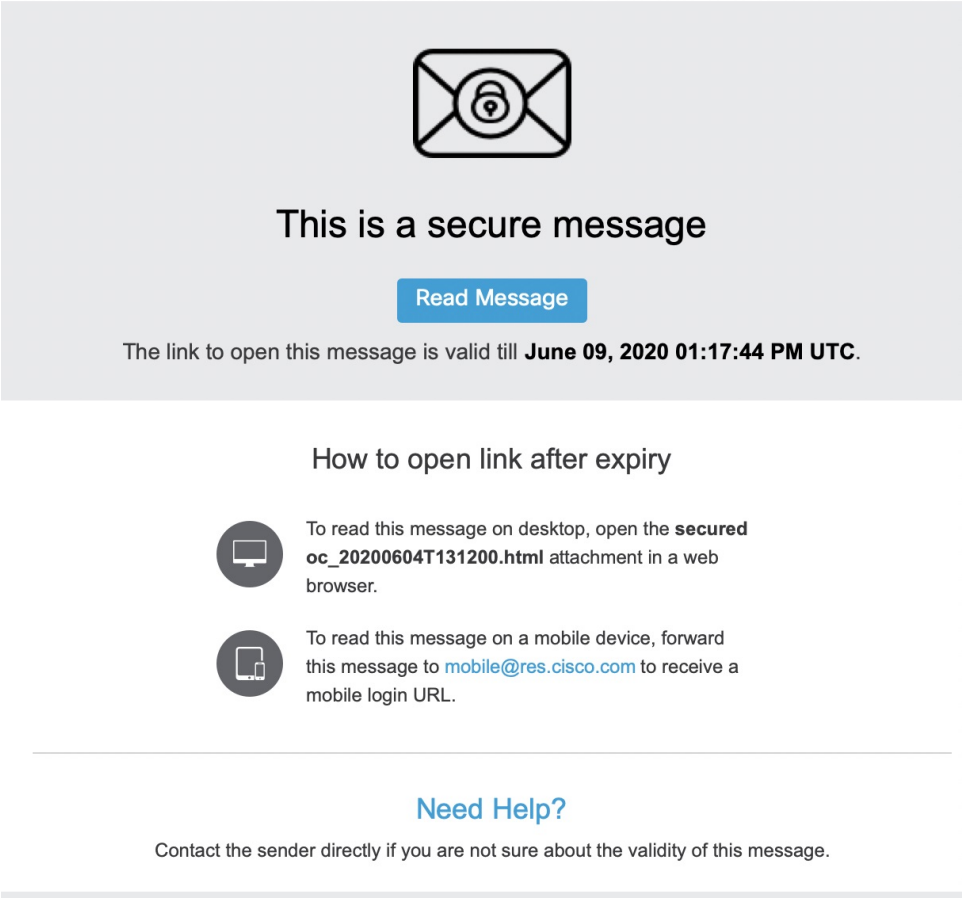
メール管理者が大容量ファイル添付のサポートを有効にしており、セキュアメッセージに 25 MB を超えるファイルが添付されている場合、securedoc html 添付ファイルはセキュアメッセージ内に表示されません。

受信した通知メッセージは、次のいずれかの方法で表示されます。

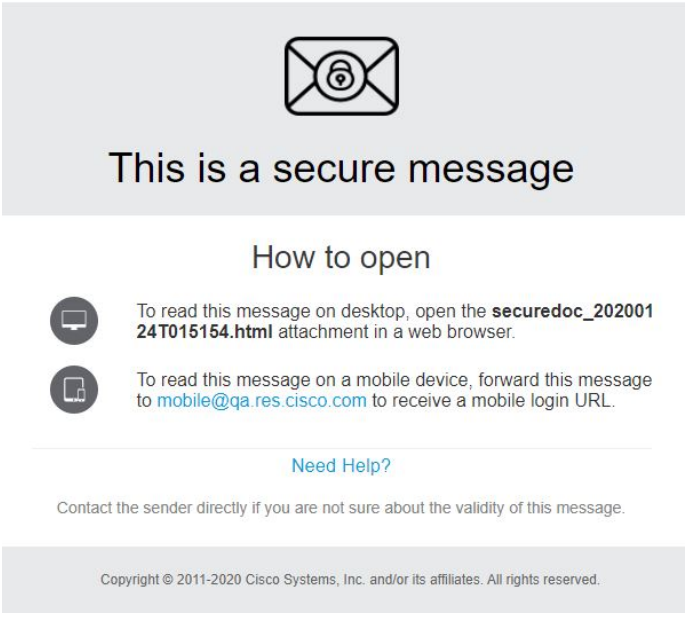
- 次の図は、[メッセージを読む（Read Message）] ボタンがある通知メールメッセージを示しています。セキュリティで保護されたメッセージを確認するには、**[Read Message]** ボタンをクリックします。デフォルトでは、**[Read Message]** リンクは最大 14 日間有効です。リンクの有効期限が切れた後は、受信者は、Web ブラウザで添付ファイルを開くか、mobile.res.cisco.com にメッセージを転送することにより、メッセージを読むことができます。



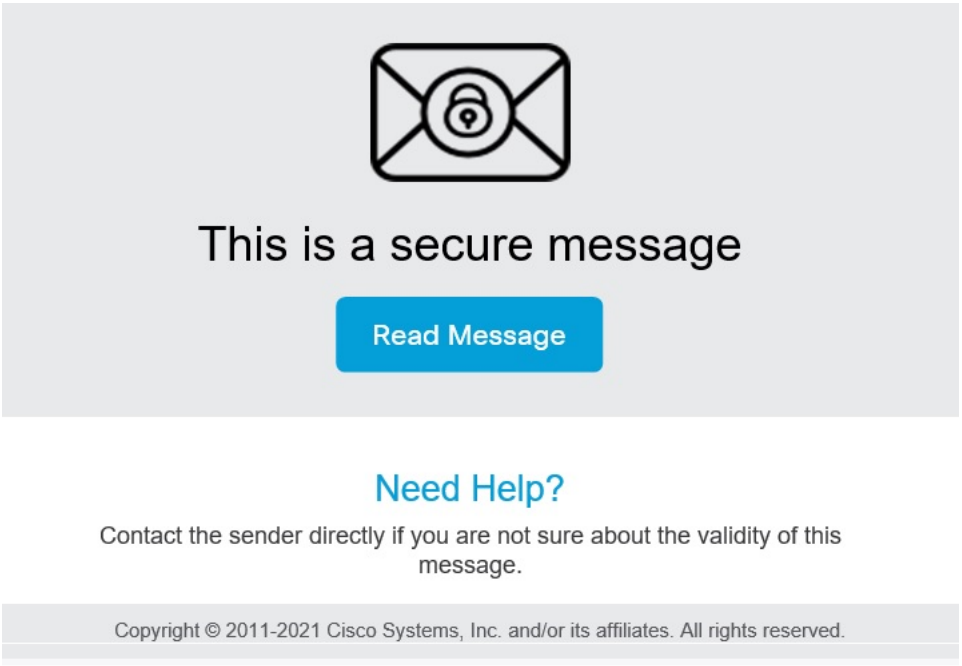
- 次の図は、[メッセージを読む（Read Message）] ボタンがある通知メールメッセージを示しています。電子メールの有効期限の月はテキスト形式で、日付はタイムスタンプ付きです。この新しい日付形式は、カスタムテンプレートにのみ適用されます。



- 次の図は、[メッセージを読む（Read Message）] ボタンのない通知メールメッセージを示しています。セキュリティで保護されたメッセージを読むには、Web ブラウザで **securedoc_dateTtime.html** 添付ファイルを開くか、mobile.res.cisco.com にメッセージを転送してください。詳細については、初めてセキュリティで保護されたメッセージを開封するための手順 （8 ページ）を参照してください。



- 次の図は、secureoc html 添付ファイルと有効期限のない通知メールを示しています。この通知タイプは、セキュアメッセージに 25 MB を超えるファイルが添付されている場合に表示されます。このような場合は、[メッセージを読む（Read Message）] ボタンをクリックしてセキュアメッセージを開きます。



（注） 添付ファイルには、ユーザーアカウントのパスワードを入力したときに暗号化されたメッセージを復号するソフトウェアが含まれます。付属するソフトウェアがメッセージを復号化できない場合があり、その場合は、代わりの復号化メソッドを使用する必要があります。セキュアメッセージを開封する際の別の方法については、セキュアメッセージに関する問題のトラブルシューティングを参照してください。

セキュアメッセージのコンポーネント

受信したセキュアメッセージの [メッセージを読む（Read message）] ボタンをクリックすると、Web ブラウザにリダイレクトされ、メッセージが表示されます。

[Secure Message] ログインページには、受信者のメールアドレスが検索可能なドロップダウンボックスに表示されます。検索可能なドロップダウンボックスを使用して、次のいずれかの方法でセキュリティで保護されたメッセージを開くことができます。

- 検索可能なドロップダウンボックスから、必要な受信者のメールアドレスを選択します。
- 検索可能なドロップダウンボックスに、受信者のメールアドレスと一致する文字を入力して、受信者のメールアドレスを検索します。

（注） Web ブラウザで JavaScript が無効になっている場合、受信者のメールアドレスは検索できません。検索可能なドロップダウンボックスでは、受信者のメールアドレスのリストを表示して選択することしかできません。

セキュアメッセージを単一の受信者に送信すると、[お客様のアドレス（Your Address）] フィールドに受信者の電子メールアドレスが自動的に入力されます。セキュアメッセージの [宛先（To）] および [コピー送信先（CC）] アドレスフィールドに複数の受信者が存在する場合、受信者のメールアドレスと一致するいずれかの文字を検索可能なドロップダウンボックスに入力すると、[お客様のアドレス（Your Address）] フィールドに自動入力されます。

（注） BCC 受信者としてセキュリティで保護されたメッセージを受信した場合は、検索可能なドロップダウンボックスから [Address Not listed] オプションを選択し、受信者のメールアドレスを手動で入力する必要があります。

すでにサービスに登録している場合は、**[Open]** ボタンが表示されます。[Open] ボタンをクリックし、コンテンツを復号してメッセージを表示します。

サービスに登録していない場合、パスワードを入力する前に、登録してユーザーアカウントを作成することを求められます。メールアドレスがユーザーアカウントに関連付けられていない場合は、メッセージに [登録（Register）] ボタンが表示されます。その場合は、**[Register]** ボタンをクリックしてサービスに登録します。

受信したメールの securedoc 添付ファイルを開くと、Web ブラウザにセキュアメッセージが表示されます。

次の表で、上の図で示されているセキュアメッセージの重要な機能について説明します。

機能	説明
アドレスフィールドと件名	アドレスフィールドでは、送信者のアドレスが [From:] フィールドに、宛先アドレスが [To:] フィールドに表示されます。
Password フィールド	セキュアメッセージがパスワードによって保護されている場合は、Encryption Service パスワードを入力してメッセージを開封します。サービスに登録していない場合は、パスワードを入力する前に登録するように求められます。
[Open] ボタン	パスワードで保護されたメッセージを受信すると、すでにサービスに登録している場合は、[Open] ボタンが表示されます。[Open] ボタンをクリックし、コンテンツを復号してメッセージを表示します。[Open] ボタンは、サービスに登録してユーザーアカウントを作成した後に初めて表示されます。メールアドレスがユーザーアカウントに関連付けられていない場合は、[開く（Open）] ボタンの代わりに [登録（Register）] ボタンが表示されます。その場合は、[Register] ボタンをクリックしてサービスに登録します。 低セキュリティのセキュアメッセージを受信した場合は、[開く（Open）] ボタンの代わりに [確認（Acknowledge）] ボタンが表示されます。 （注） 企業によっては、Cisco Secure Message Service でシングルサインオン（SAML）ログインが使用できるよう設定されている場合があります。その場合は、企業の資格情報を使用してログインするためのポップアップが表示されます。
[Sign in with Google] ボタン	Google アカウントがある場合は、**[Google Sig-up]** ボタンをクリックして登録する必要があります。登録すると、Google でサインインしてセキュリティで保護されたメッセージを確認できるようになります。この場合、Encryption Service に登録したり、Encryption Service パスワードを入力したりする必要はありません。
[Help] リンク	[ヘルプ（Help）] リンクをクリックし、セキュアメッセージのオンラインヘルプにアクセスします。オンラインヘルプでは、セキュアメッセージを開封するための標準的な方法および代替方法について説明します。よく寄せられる質問（FAQ）へのリンクもあります。
メッセージのセキュリティレベル	メッセージのセキュリティレベルは、低、中、または高に設定できます。デフォルトは medium です。低セキュリティで送信されたメッセージを開くには、パスワードを入力する必要はありません。中セキュリティでは、標準のパスワード機能を使用できます。高セキュリティで送信されたメッセージを開封するには、[Remember me on this computer] オプションをオンにしている場合にも、必ずパスワードを入力する必要があります。

機能	説明
[Remember Me] チェックボックス	[Remember me on this computer] チェックボックスをオンにすると、設定内容がコンピュータに記録されます。この設定は、暗号化プロファイルによって異なります。たとえば、中セキュリティのメッセージを受信した場合は、開封のためにパスワードを入力する必要がない場合もありますが、高セキュリティのメッセージを受信した場合は、開封のために必ずパスワードを入力する必要があります。
言語	受信するセキュアメッセージの翻訳に使用する言語を選択します。この選択により、BCE設定ファイルに設定されたシステムのデフォルトロケールによって決定される言語が上書きされます。
ロゴ	Encryption Service アプリケーションの [アカウント管理（Account Management）] > [ブランディング（Branding）] > [イメージ（Images）] ページに、エンベローププロファイル用に選択したカスタムロゴが表示されます。

セキュアメッセージのその他の機能については、次のアドレスから「よく寄せられる質問（FAQ）」をご覧ください。

https://res.cisco.com/websafe/help?topic=FAQ

セキュアメッセージのほとんどの構成要素はメッセージごとに異なります。エンベロープの構成要素に影響を与える要因には以下が挙げられます。

- 送信者のアカウント設定。
- 受信者のコンピュータにインストールされているソフトウェア。
- 電子メールゲートウェイによって、暗号化されたメッセージの添付ファイルに追加された変更。
- 受信者がすでにサービスに登録済みかどうか。

セキュアメッセージは動的であり、特定のメッセージの構成要素は時間の経過によって変化する可能性があります。

初めてセキュリティで保護されたメッセージを開封するための手順

このセクションでは、パスワード保護されたセキュアメッセージを初めて開封する方法について詳しく説明します。この手順は、初めて受信した場合の標準的なシナリオです。手順は状況によって異なる場合があります。Google アカウントがある場合は、Google 認証を使用してセキュリティで保護されたメッセージを開くことができます。詳細については、Google サインインによりセキュリティで保護されたメッセージを開く （13 ページ）を参照してください。

（注） これらの手順は、パスワードで保護されたメッセージを初めて受信したユーザーのみに適用されます。Encryption Service に登録してアカウントを有効化すると、パスワードを使用して、どの送信者からのセキュアメッセージでも開けるようになります。パスワードによって保護されていないセキュアメッセージを受信した場合、メッセージの開封のために登録する必要はありません。詳細については、Encryption Service アカウントの有効化後にセキュアメッセージを開く （13 ページ）を参照してください。

最初のセキュアメッセージを開くには、次の手順を実行する必要があります。

（注） セキュアメッセージに 25 MB を超えるファイルが添付されている場合、securedoc html 添付ファイルはセキュアメッセージ内に表示されません。このような場合は、セキュアメッセージ上にある [メッセージを読む（Read Message）] ボタンをクリックして、下記の手順 3 から開始します。

手順

ステップ 1 暗号化されたメッセージの添付ファイルをハードドライブに保存する （9 ページ）
ステップ 2 ファイルを Web ブラウザで開く （10 ページ）
ステップ 3 [Register] ボタンをクリックして Cisco Registered Envelope Service に登録する （10 ページ）
ステップ 4 Encryption Service アカウントの有効化 （12 ページ）
ステップ 5 セキュアメッセージの再表示とパスワードの入力 （12 ページ）

暗号化されたメッセージの添付ファイルをハードドライブに保存する

セキュアメッセージの通知を受け取った場合、添付ファイル（securedoc_*date*T*time*.html。*date* と *time* は、メールの送信時に付加されたタイムスタンプを表します）をダウンロードして、ファイルを開く前にハードドライブに保存する必要があります。

（注） 添付ファイルを保存するためのダイアログボックスは、お使いの電子メールプログラムや Web メールサイト（Yahoo! メール、Gmail、Hotmail）によって異なる場合があります。

通知メッセージの詳細については、セキュアメッセージの通知 （2 ページ） を参照してください。

ファイルを Web ブラウザで開く

Web ブラウザで securedoc_*date* T*time* .html ファイル（ダウンロードしたファイルの保存先から）を開きます。

（注） 電子メールの添付ファイルから直接ファイルを開かないでください。最初にファイルをシステムにダウンロードし、ダウンロードしたファイルの保存先から html ファイルを開く必要があります。

セキュアメッセージに登録ページが表示されます。

[Register] ボタンをクリックして Cisco Registered Envelope Service に登録する

セキュアメッセージを開くには、Cisco Secure Email Encryption Service にアカウントを登録する必要があります。

（注） 企業によっては、Encryption Service でシングルサインオン（SAML）認証が使用できるよう設定されている場合があります。その場合は新規ユーザー登録が簡略化され、ポータル言語と Encryption Service ユーザーアカウントに使用する名前のみ入力する必要があります。次の図は、SAML 認証による新規ユーザー登録を示しています。

[新規ユーザー登録（New User Registration）] ページが表示されます。

（注） [新規ユーザー登録（New User Registration）] ページでは、アカウントを Cisco Secure Message Service に登録するまで、カスタマイズされたロゴとフッターリンクを表示できません。

（注） 新しいアカウントの登録時に、セキュリティに関する質問と個人のセキュリティに関するフレーズは不要になりました。

次のフィールドに情報を入力します。

表 *1 : Encryption Service* 登録ページのフィールド

フィールド	値
First Name	必須です。Encryption Service ユーザーアカウントの名前（名）を入力します。

フィールド	値
Last Name	必須です。Encryption Service ユーザーアカウントの名前（姓）を入力します。
Password および Confirm Password	必須です。アカウントのパスワードを入力し、再度確認入力します。パスワードは英数字を使用し、大文字と小文字を区別する必要があります。 次のパスワード要件は、アカウント管理者が追加の設定を行うことができます。 • パスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字タイプが含まれる必要があります。 • パスワードには 3 回以上連続して繰り返される文字を含めることはできません。 • パスワードにはユーザー名または反転したユーザー名を含めることはできません。 • パスワードには「Cisco」、「ocsic」の文字列を使用することはできません。また、同様の文字列の大文字/小文字を変更したものや、「i」を「1」、「|」、「!」に置き換えたもの、「o」を「0」に置き換えたもの、「s」を「$」に置き換えたものも使用できません。 （注） パスワードを忘れた場合は、セキュアメッセージの [パスワードを忘れた場合（Forgot Password?）] ボタンをクリックして、パスワードをリセットします。 企業が Cisco Secure Message Service でシングルサインオン（SAML）ログインを使用できるよう設定している場合には、企業のサポートグループに問い合わせてパスワードを入手またはリセットしてください。
Encryption Service の利用規約に同意します	Encryption Service でアカウントを登録するには、このチェックボックスをオンにする必要があります。

（注） ダイナミックなパスワード検証では、アカウント管理者が Encryption Service に対して設定した追加のパスワードルールについては検証が行われません。

登録時に、次のアカウント アクティベーション ページが表示されます。Encryption Service アカウントを有効化するには、アカウント アクティベーション メールの指示に従う必要があります。

（注） 複数のメールアドレスでセキュアメッセージを受信する場合、複数のユーザーアカウントを設定する必要が生じることがあります。各メールアドレスには個別のユーザーアカウントが必要です。

Encryption Service アカウントの有効化

受信トレイにアカウント有効化のメッセージがサービスから届いているかを確認してください。受信トレイに電子メールが届いていない場合は、アカウント有効化のメッセージがフィルタされている可能性があるため、迷惑メールフォルダを確認してください。

アカウント有効化メールメッセージで、リンクをクリックしてユーザーアカウントを有効にします。

セキュアメッセージの再表示とパスワードの入力

手順

ステップ 1 セキュアメッセージに戻ります。[登録（Register）]ボタンは、メッセージに表示されなくなります。代わりに、[開く（Open）] ボタンが表示されます。

ステップ 2 Cisco Secure Message Service のユーザーアカウントのパスワードを入力し、[開く（Open）] をクリックします。

（注） 企業によっては、Cisco Secure Message Service でシングルサインオン（SAML）ログインが使用できるよう設定されている場合があります。その場合は、企業の資格情報（ユーザー名とパスワード）を使用してログインし、暗号化された電子メールを認証し開くためのポップアップが表示されます。Google アカウントでサインインする場合は、セキュリティで保護されたメッセージを確認するために Encryption Service のユーザー名とパスワードを入力する必要はありません。

復号されたメッセージがブラウザウィンドウに表示されます。

ステップ 3 セキュアメッセージを開封すると、[返信（Reply）] をクリックしてセキュリティで保護された返信メッセージを送信するか、[転送（Forward）] をクリックしてセキュリティで保護された転送メッセージを送信できます。セキュリティで保護された返信メッセージまたは保護された転送メッセージを送信すると、受信者は暗号化されたメッセージを含むセキュアメッセージを受信します。

（注） オリジナルメッセージの送信者の設定によって、特定の機能が使用できない場合があります。たとえば、セキュリティで保護されたメッセージを返信または転送できない場合があります。

Encryption Service アカウントの有効化後にセキュアメッセージを開く

Cisco Secure Message Service に登録してアカウントを有効化すると、Encryption Service パスワードを使用して、どの送信者からのセキュアメッセージでも開けるようになります。

セキュアメッセージを開封するときに Encryption Service パスワードを忘れた場合は、セキュアメッセージの [パスワードを忘れた場合（Forgot Password?）] ボタンをクリックして、パスワードをリセットします。アカウントに関連付けられているメールアドレスに新しいパスワードのメッセージが送信されます。

新しいパスワードメッセージには *[Create New Password]* ページへのリンクが表示されます。このリンクをクリックすると、新しいパスワードを作成するためのブラウザにリダイレクトされます。アカウントにログインしてセキュアメッセージを開封する際、ここで設定したパスワードを使用します。パスワードをリセットするたびに、Encryption Service アカウントに関連付けられているメールアドレスに通知メールが送信されます。パスワードをリセットするためのセキュリティに関する質問は不要になりました。

（注） 企業が Cisco Secure Message Service でシングルサインオン（SAML）ログインを使用できるよう設定している場合には、企業のサポートグループに問い合わせてパスワードを入手またはリセットしてください。

Google サインインによりセキュリティで保護されたメッセージを開く

Google アカウントがある場合は、Google 認証を使用してセキュリティで保護されたメッセージを開くことができます。この場合、セキュアメッセージを開封するために Encryption Service に登録したり、Encryption Service パスワードを入力したりする必要はありません。

最初に Google 認証によりセキュリティで保護されたメッセージを開く方法：

手順

ステップ 1 添付の **securedoc.html** ファイルをシステムにダウンロードします。

ステップ 2 ファイルが保存されている場所に移動し、Web ブラウザでファイルを開きます。

（注） セキュアメッセージに 25 MB を超えるファイルが添付されている場合、securedoc html 添付ファイルはセキュアメッセージ内に表示されません。このような場合は、セキュアメッセージ上にある [メッセージを読む（Read Message）] ボタンをクリックします。

ステップ 3 **[Google Sign-up]** ボタンをクリックして登録します。

ステップ 4 Google アカウントを選択します。

ステップ 5 **[New Google User Registration]** ページで、姓と名を入力し、**[Register]** をクリックします。

確認メッセージが表示されます。電子メール宛てに確認が送信されます。

ステップ 6 セキュアメッセージに戻り、[Googleでサインインする（Sign in with Google）] ボタンをクリックしてセキュリティで保護されたメッセージを確認します。

（注） **[パスワード（Password）]** フィールドは、Encryption Service 認証でのみ必要となります。Google サインインによりセキュリティで保護されたメッセージを開く場合は、**[Password]** フィールドは使用しません。このフィールドはスキップして、**[Sign in with Google]** をクリックします。