



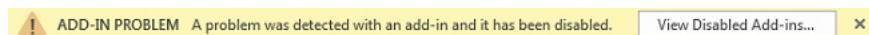
Cisco Secure Email Encryption Plug-in for Outlook の設定と使用

この章では、Cisco Secure Email Encryption Plug-in for Outlook で使用可能な機能について説明します。Cisco Secure Email Encryption Plug-in には Outlook 電子メールプログラムと連動するいくつかのタイプのプラグインが用意されています。

- [Cisco Secure Email Encryption Plug-in の有効化](#) (1 ページ)
- [使用状況データ収集の設定](#) (2 ページ)
- [Cisco Secure Email Encryption Plug-in for Outlook の全般設定](#) (3 ページ)
- [Outlook プラグインの基本設定](#) (4 ページ)
- [更新をチェックするための Outlook Plug-in の設定](#) (5 ページ)
- [BCE_Config ファイルを使用した共通オプションの設定](#) (7 ページ)
- [暗号化メッセージのストレージオプションの設定](#) (8 ページ)
- [セキュアメッセージのオープン](#) (9 ページ)
- [電子メールの暗号化](#) (11 ページ)
- [Flag およびデスクトップ暗号化の設定](#) (12 ページ)
- [Flag 暗号化](#) (14 ページ)
- [Desktop Encryption](#) (18 ページ)
- [追加設定の変更](#) (37 ページ)
- [エラーとトラブルシューティング](#) (40 ページ)
- [診断ツールを使用したトラブルシューティング](#) (43 ページ)
- [エンベロープでの JavaScript の無効化](#) (47 ページ)
- [Cisco Secure Email Encryption Plug-in のアンインストール](#) (48 ページ)

Cisco Secure Email Encryption Plug-in の有効化

インストール後に初めて Cisco Secure Email Encryption Plug-in を起動すると、Outlook によって無効にされることがあります。無効になっている場合には、次のメッセージが表示されます。



Cisco Secure Email Encryption Plug-in を有効にするには、通知バーの [View Disabled Add-ins] ボタンをクリックして [Disabled Add-ins] ダイアログを表示します。起動時にどれだけ時間がかかっても必ずアドインが実行されるように Outlook を設定するには、[Always enable this add-in] ボタンをクリックします。

使用状況データ収集の設定

Cisco Secure Email Encryption Plug-in を最初に起動すると、製品の改善に役立てるために匿名データをシスコに送信できるようにするかどうかを尋ねられます。[Send anonymous usage data to Cisco] チェックボックスをオンにすると、次の2つのタイプの情報が収集され、分析するために Cisco サーバーに保存されます。

- プラグインを実行しているマシンに関する一般情報
- アカウント固有の情報

以下では、この情報の詳細について説明します。

起動後に [プラグインオプション (Plug-in Options)] > [追加オプション (Additional Options)] > [使用状況を送信する (Sending usage data)] タブを選択し、使用率データの送信を有効または無効にすることができます。

使用状況データのシスコへの送信を有効または無効にするには、CommonComponentsConfig.xml ファイルで次のパラメータを設定します。

- `callHomeAdminEnabled` : Outlook を起動したときに使用状況データの送信を有効にするには `true` を、送信を無効にするには `false` を設定します。デフォルト値は `true` です。 `false` に設定すると、使用状況データ収集に関する通知を受信できず、シスコに匿名の使用状況データを送信することができなくなります。

一般情報

次の情報が収集されます。

- 識別子 (UUID) : プラグインを最初にインストールするときに生成される非永続的な識別子。使用状況データが時系列で追跡する使用状況レポートを関連付ける目的でのみ使用します。[Plug-in Options] > [Additional Options] > [Privacy] タブを選択すると、識別子をリセットすることができます。
- オペレーティング システムのバージョン
- Microsoft Outlook のバージョン
- Cisco Outlook Plug-in のバージョン
- Cisco Encryption SDK のバージョン : この SDK は、セキュリティで保護されたメッセージの暗号化と復号化のためにプラグインが内部で使用するライブラリです。
- オペレーティング システムで使用される言語

- インストールされたすべての Outlook プラグインの名前

アカウント固有の情報

次の情報が収集されます。

- アカウント タイプ：タイプは暗号化、復号化、またはフラグのいずれかです。
- サーバ
- 受信者数：インストールされてから暗号化中に追加された受信者の数。フラグ設定中に追加された受信者も含まれます。
- 復号化カウント：プラグインを使用して復号化されたメッセージの数。
- 暗号化カウント：インストールされてからデバイスで暗号化されたメッセージの数。フラグが付けられたメッセージの数も含まれます。
- メッセージの管理カウント：[メッセージの管理] 画面へのアクセス回数。
- メッセージの管理の使用数：[Manage Messages] 画面を使用して更新されたメッセージの数。

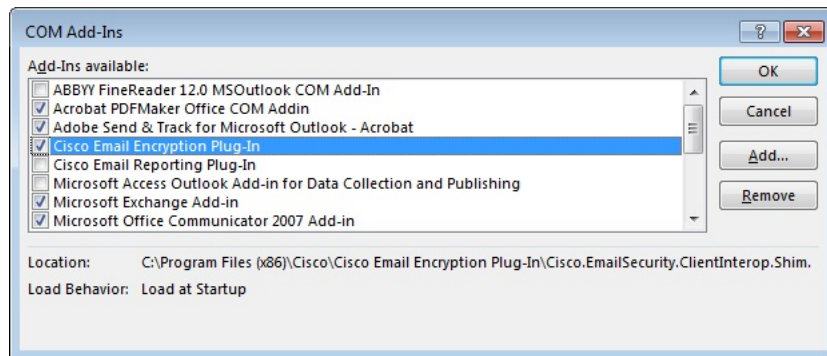
Cisco Secure Email Encryption Plug-in for Outlook の全般設定

Cisco Secure Email Encryption Plug-in の全般設定は、[Options] ページから行えます。

Enable または Disable

デフォルトでは、Cisco Secure Email Encryption Plug-in はインストール時に有効になります。Cisco Secure Email Encryption Plug-in は次の場所から無効にできます。

- Outlook 2010/2013/2016 では、[File] > [Options] に移動し、左側のナビゲーションバーから [Add-ins] を選択します。次に、ページの下部にある [Manage] ドロップダウンメニューから [COM Add-ins] を選択し、[Go...] をクリックします。
- Outlook 2007 では、[Tools] > [Trust Center] に移動し、左側のナビゲーションバーから [Add-ins] を選択します。次に、ページの下部にある [Manage] ドロップダウンから [COM Add-ins] を選択し、[Go] をクリックします。



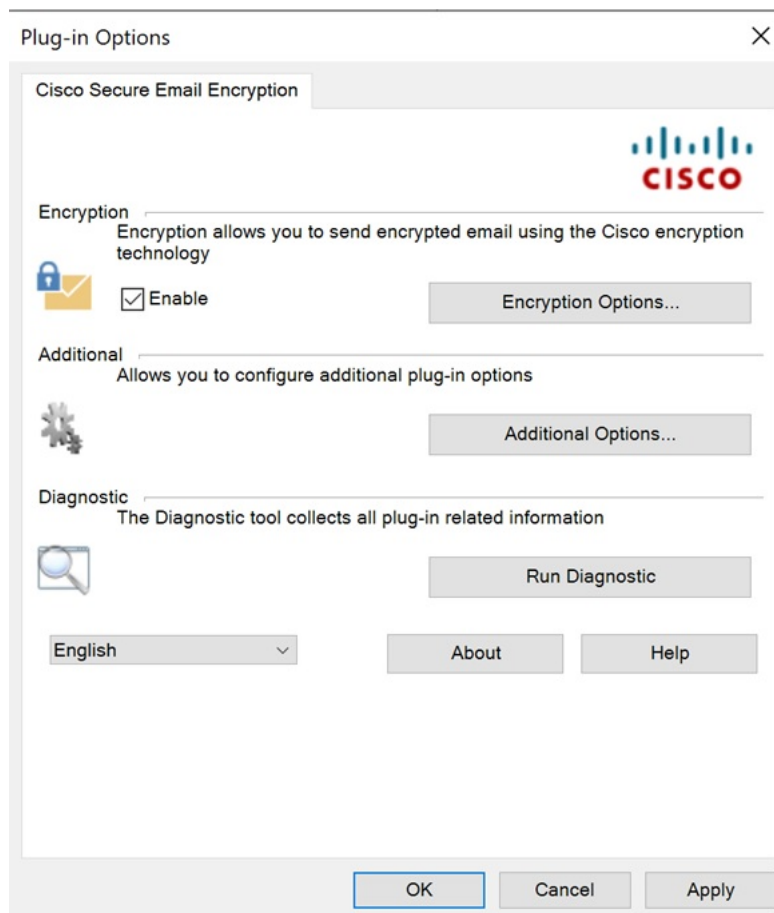
[COM Add-Ins] ウィンドウで、[Cisco Secure Email Encryption Plug-in] チェックボックスをオフにして [OK] をクリックします。

Outlook プラグインの基本設定

エンドユーザーは [Cisco Secure Email Encryption] タブで基本的な設定項目を設定できます。

- Outlook 2010/2013/2016 では、リボンの [Plug-in Options] ボタンをクリックするか、または [File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Encryption] に移動します。
- Outlook 2007 では、ツールバーの [Plug-in Options] ボタンをクリックするか、または [Tools] > [Options] > [Cisco Email Security Encryption] に移動します。

[Cisco Secure Email Encryption] タブ :



エンドユーザーは、このタブで [Enable] チェックボックスをオンにすることにより、暗号化のオプションを有効にできます。エンドユーザーは、[Additional Options] ボタンを選択して、その他のオプションを有効にすることができます。詳細な設定を行うには、[Encryption Options] または [Additional Options] ボタンをクリックします。エンドユーザーは、問題解決時に診断ツールを使用し、Cisco Secure Email Encryption Plug-in でレポートを実行してシスコのサポートに送信することもできます。Outlook を起動したときに、匿名の使用情報 (Plug-in の使用に関する一般情報) をサーバーへ送信するように Plug-in を設定することもできます。

更新をチェックするための Outlook Plug-in の設定

更新を自動でチェックするようにプラグインを設定するには、CommonComponentsConfig.xml ファイルの checkForUpdates セクションで次のパラメータを設定します。

- **checkAutomatically** : Outlook を起動したときに更新の自動チェックを有効にするには true を、無効にするには false を設定します。デフォルト値は true です。
- **serverURL** : 新しいバージョンを利用できるかどうかをチェックするためにプラグインで使用する URL を設定します。
- **ignoredVersion** : 更新を探すときに、プラグインで無視するバージョン番号を設定します。

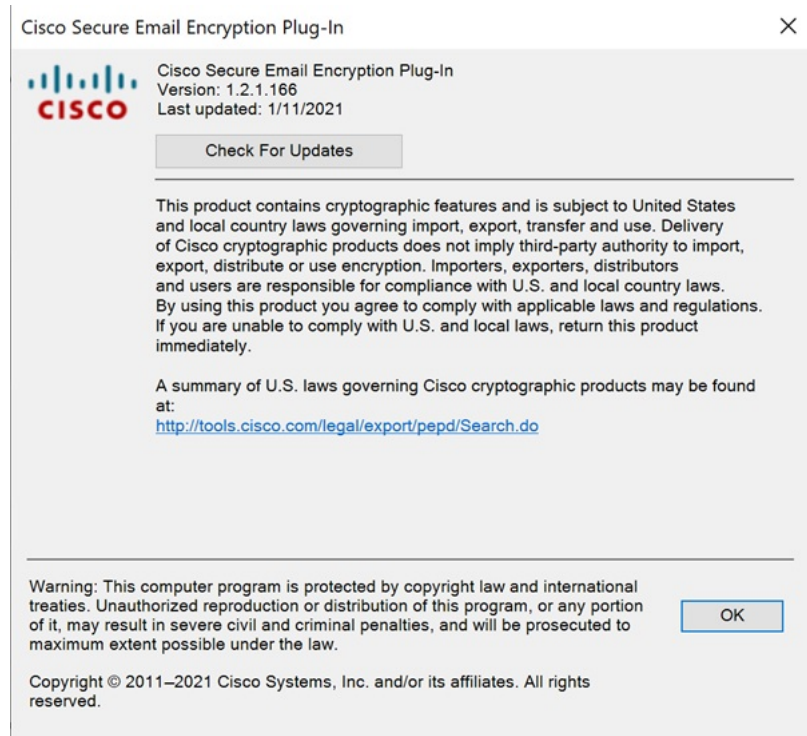
更新の通知

Desktop Encryption プラグインで更新を自動的にチェックするように設定されており、Desktop Encryption プラグインの現在のバージョンが最新ではない場合は、Outlook の起動時に次のダイアログボックスが表示されます。



- (注) Cisco Secure Email Encryption Plug-in アプリケーションをダウンロードするための適切な権限が必要です。

Outlook を起動した後で更新をチェックするには、[Plug-in Options] ウィンドウの [About] ボタンをクリックし、次のダイアログボックスで [Check for updates] ボタンをクリックします。



BCE_Config ファイルを使用した共通オプションの設定

すべての Outlook アカウントおよびプラグイン全体で共通のオプションは、CommonComponentsConfig.xml ファイルに含まれています。これらのオプションを次に示します。

- **diagnosticSupportAddress** : 診断ツールを実行したときに送信されるメッセージの受信者の電子メール アドレスを指定します。メッセージには、診断ツールの出力が含まれます。
- **diagnosticReportSubject** : 診断ツールを実行したときに送信されるメッセージの件名を指定します。
- **showPluginOptions** : 暗号化、診断、追加オプションを実行できる [Plug-in Options] ダイアログボックスを開く [Plug-in Options] ボタンを有効にするには **true** に、無効にするには **false** に設定します。 **false** を設定すると、[Plug-in Options] ボタンは表示されません。
- **showManageMessageButton** : メッセージをロックしたり、メッセージの有効期限を設定できる [Manage Messages] ダイアログボックスを開く [Manage Messages] ボタンを有効にするには **true** に、無効にするには **false** に設定します。 **false** を設定すると、[Manage Messages] ボタンは表示されません。
- **checkAutomatically** : Outlook を起動したときに更新の自動チェックを有効にするには **true** を、無効にするには **false** を設定します。デフォルト値は **true** です。詳細については、[更新をチェックするための Outlook Plug-in の設定 \(5 ページ\)](#) を参照してください。

- **serverURL** : 新しいバージョンを利用できるかどうかをチェックするためにプラグインで使用する URL を設定します。
- **callHomeAdminEnabled** : Outlook を起動したときに使用状況データの送信を有効にするには **true** を、送信を無効にするには **false** を設定します。デフォルト値は **true** です。false に設定すると、使用状況データ収集に関する通知を受信できず、シスコに匿名の使用状況データを送信することができなくなります。詳細については、[使用状況データ収集の設定 \(2 ページ\)](#) を参照してください。
- **callHomeEnabled** : Outlook を起動したときに使用状況データの送信を有効にするには **true** を、送信を無効にするには **false** を設定します。デフォルト値は **true** です。false に設定すると、ユーザーは匿名の使用状況データをシスコに送信できません。詳細については、[使用状況データ収集の設定 \(2 ページ\)](#) を参照してください。

これらのオプションが **BCE_Config.xml** ファイルに設定されている場合は、プラグインが **BCE_Config.xml** を適用すると、オプションが **CommonComponentsConfig.xml** にコピーされます。それ以外の場合、これらのオプションをユーザー環境で変更するには、**UseCustomConfig** オプションで多数のインストールを実行する必要があります。詳細は、[BCE_Config.xml ファイルによる一括インストールのセクション](#)を参照してください。

同様に、**BCE_Config** を適用して、アカウント固有のファイル (**config_1.xml**、**config_2.xml** など) でオプションを設定することもできます。ただし、**BCE_Config.xml** ファイルを使用してロギングの設定、またはプラグインのローカリゼーションを設定することはできません。

BCE_Config.xml のパラメータの詳細については、[BCE_Config.xml のパラメータ](#)を参照してください。

暗号化メッセージのストレージオプションの設定

[メッセージからの読み取り (Read from Message)] 機能 (旧 Easy Open) を使用すると、受信者は、クライアント側のアプリケーションをインストールすることなく、どのデバイスからでもエンベロープを開封することができます。これは、エンベロープを受信者への添付ファイルとして送信することに加えて、Cisco Secure Email Encryption Service または外部ストレージに暗号化されたメッセージのコピーを保存することによって実現できます。

有効になっている場合は、[メッセージを読む (Read Message)] ボタンを備えた新しいテンプレートにセキュアメッセージが表示されます。受信者がこのボタンをクリックすると、その受信者は、セキュアメッセージを認証して復号するように指示されます。



重要 [メッセージを読む (Read Message)] のサポートは、Cisco Secure Email Gateway (ESA) 11.1.0-302、11.1.3-006、および 12.x (一般的な導入) 以降のリリースで利用できます。

外部ストレージの設定

この機能が有効になっている場合、暗号化されたエンベロープのコピーを保存する優先ストレージを設定できます。次のストレージオプションを使用できます。

- Cisco ストレージ
- Microsoft OneDrive ストレージ



(注) 大きな添付ファイル用に OneDrive ストレージを使用しているときに、セキュアメッセージに [メッセージを読む (Read Message)] ボタンを表示するには、Microsoft Office365 アプリケーションに *files.write* および *file.readwrite* API 権限が存在している必要があります。

Cisco Secure Email Encryption Plug-in でメッセージからの読み取りと外部ストレージを設定するには、『[Cisco Secure Email Encryption Service Account Administrator Guide](#)』を参照してください。

Cisco Secure Email Encryption Plug-in で Easy Open 機能を設定した後に、[セキュアメッセージのオープン \(9 ページ\)](#) を参照してください。

セキュアメッセージのオープン

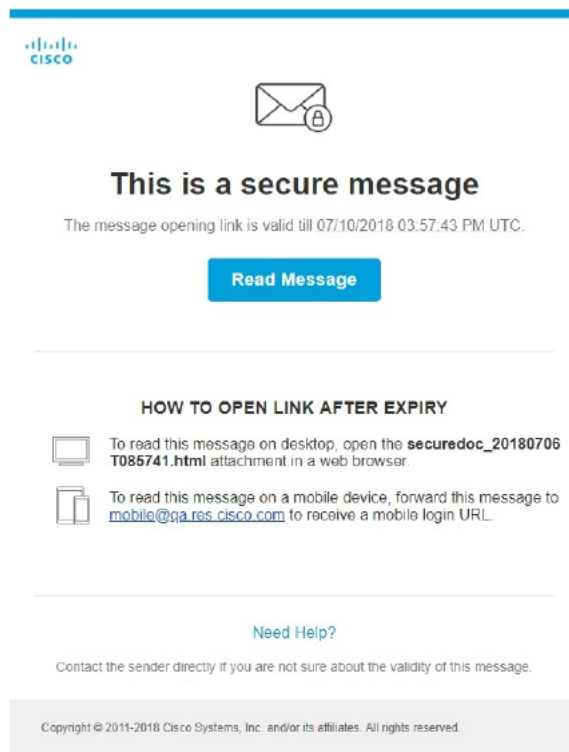
Cisco Secure Email Encryption Service にユーザーアカウントを登録して、セキュアなメッセージを開くには、次の手順を実行します。



(注) アカウントで Easy Open を有効にしている場合は、[Read Message] ボタンと securedoc HTML 添付ファイルを通知メールメッセージに表示できます。

手順

-
- ステップ 1** セキュアメッセージを読むには、通知メールメッセージの [Read Message] ボタンをクリックします。



- ステップ 2** メールボックスのセキュアメッセージをダブルクリックします。[Register] ボタンが付いた [Decryption] ダイアログが表示されます。
- ステップ 3** [Email Address] ドロップダウンメニューから電子メールアドレスを選択し、[Register] をクリックします。[New User Registration] ページが開きます。
- (注) 複数のメールアドレスで登録済みエンベロープを受信する場合は、複数のユーザーアカウントを設定する必要があります。電子メールアドレスごとに個別のユーザーアカウントが必要です。
- ステップ 4** フォームに入力して、[Register] をクリックします。
- ステップ 5** 受信箱フォルダにアカウントのアクティベーションメッセージが届いていないか確認します。電子メールのアクティベーションリンクをクリックします。
- ステップ 6** 元の電子メールに戻り、セキュアメッセージをダブルクリックします。
- ステップ 7** [Password] フィールドに Encryption Service を入力し、[OK] をクリックしてセキュアメッセージを読み取ります。

次のタスク

[暗号化されたセキュアメッセージを初めて開封する場合 \(11 ページ\)](#)

暗号化されたセキュアメッセージを初めて開封する場合

暗号化されたセキュアメッセージを受信した場合、その暗号化されたメッセージを開くには、Cisco Secure Email Encryption Service に登録し、ユーザーアカウントを設定する必要があります。サービスに登録した後は、アカウントのパスワードを使用することで、受信したすべての暗号化メッセージを開くことができます。

新規ユーザー登録のオプション

フィールド	説明
Language	オプション。ドロップダウンメニューから、Encryption Service アカウントで使用する言語を選択します。登録ページはデフォルトでは英語で表示されますが、日本語、英語、フランス語、ドイツ語、スペイン語、ポルトガル語から選択できます。
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。
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	必須です。アカウントのパスワードを入力します。パスワードは8文字以上とし、数字とアルファベットの両方を含める必要があります。

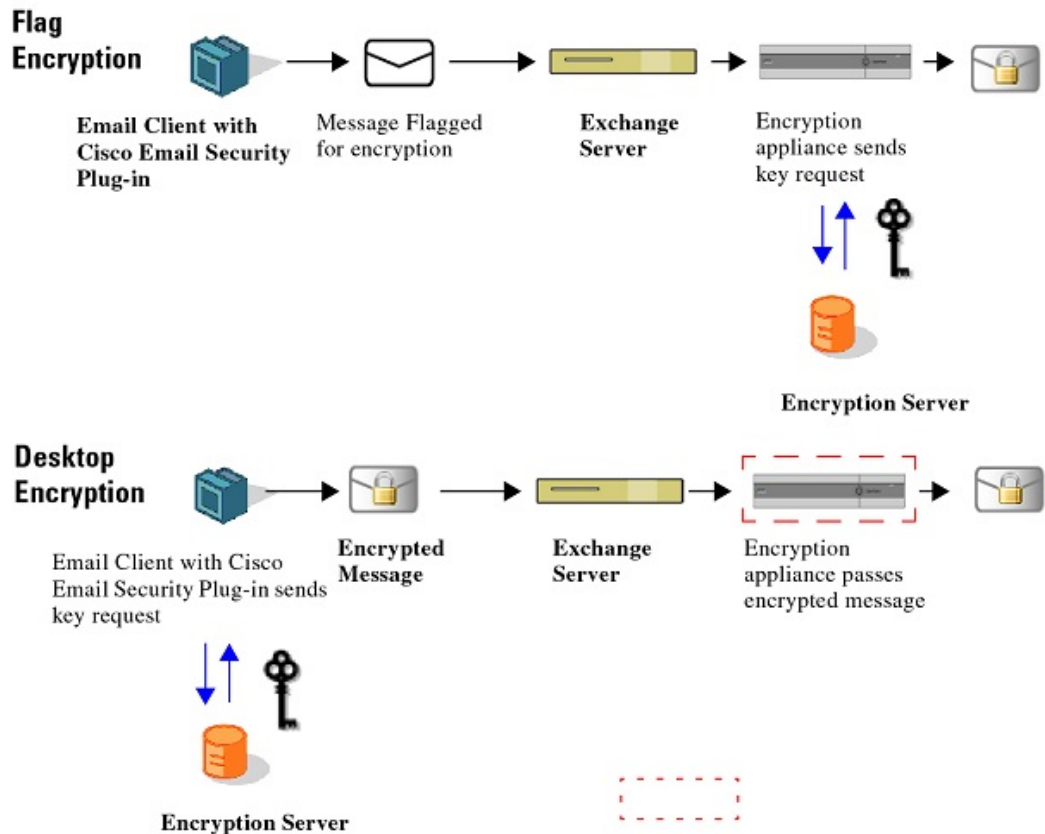
電子メールの暗号化

暗号化プラグインを使用すると、エンドユーザーは企業ネットワークの外部に電子メールを送信する前に、デスクトップからメールを暗号化したり、暗号化が必要な電子メールにフラグを設定することができます。次のいずれかの暗号化オプションを選択します。

- Flag 暗号化。** Flag 暗号化オプションを使用すると、エンドユーザーは暗号化に必要なフラグを設定できます。また、Cisco Secure Email Gateway によって電子メールが暗号化されてから電子メールがネットワークの外部に送信されます。Flag 暗号化は、エンドユーザーが組織外に送信するメールを暗号化する必要があり、組織内で送信するメールの暗号化を必要としない場合に使用できます。たとえば、機密の医療文書を扱っている組織では、患者に送信する前にそれらの文書を暗号化する必要があります。
- デスクトップ暗号化。** デスクトップ暗号化では、Cisco 暗号化テクノロジーを使用して Outlook 内から電子メールを暗号化できます。その後、暗号化された電子メールがデスクトップから送信されます。デスクトップ暗号化は、エンドユーザーが組織内で送信する

メールを暗号化する必要がある場合に使用できます。たとえば、組織内と組織外の両方の送信において、すべての機密財務データを暗号化する必要がある場合などです。

図 1: Flag 暗号化とデスクトップ暗号化のワークフロー



(注) 暗号化の方式は、Outlook 電子メールアカウントから、署名された BCE Config 添付ファイルを復号化することによって決まります。デフォルトでは、Decrypt Only モードが有効になります。エンドユーザーは、管理者から更新済みの署名された BCE Config ファイルを受信して復号化することによって暗号化方式を変更できるように、インストールを変更できます。

Flag およびデスクトップ暗号化の設定

エンドユーザーの Outlook 電子メールアカウントのデフォルトのコンフィギュレーションモードは、Decrypt Only です。フラグまたは暗号化機能を有効にするには、更新済みの添付ファイルを管理者から受け取り、それを使用してエンドユーザーの電子メールアカウントを設定し

ます。また、フラグおよび暗号化機能は一括インストールによって有効化できます。一括インストールでは、一連のコンフィギュレーションファイルがユーザーの設定フォルダに直接配布されます。復号化したメッセージに、署名された BCE 構成添付ファイルが含まれている場合は、エンドユーザーがその構成ファイルを起動すると、Encryption Plug-in for Outlook が自動的に設定されます。Cisco Secure Email Encryption Service はキーサーバーとして使用されます。エンドユーザーがアカウントを持っていない場合は、登録を求めるプロンプトが表示されます。

次の3つのコンフィギュレーションモードを利用できます。

- **Decrypt Only** : 受信した暗号化電子メールを復号化できます。
- **Decrypt and Flag** : 安全な電子メール メッセージの復号化とフラグ設定を行うことができます。flag オプションを使用すると、エンドユーザーは暗号化に必要なフラグを設定できます。また、Cisco Secure Email Gateway によって電子メールが暗号化されてから電子メールがネットワークの外部に送信されます。フラグが設定されたメッセージを検出してサーバーで復号化できるようサーバーの設定を行う必要があります。
- **Decrypt and Encrypt** : 安全な電子メール メッセージの暗号化と復号化を行うことができます。

Encryption Plug-in 構成ファイルの起動

エンドユーザーは、Outlook 電子メールアカウントから、署名された BCE Config 添付ファイルを復号化することによって、Outlook 電子メールアカウントの暗号化を有効化したり設定することができます。エンドユーザーの受信トレイに添付ファイル付きの通知メールがない場合は、スパム メールまたは迷惑メールのフォルダを調べてください。

コンフィギュレーション ファイルを起動すると、署名された BCE Config 添付ファイル付きの通知メッセージを受信した電子メールアカウントにプラグインが設定されます。

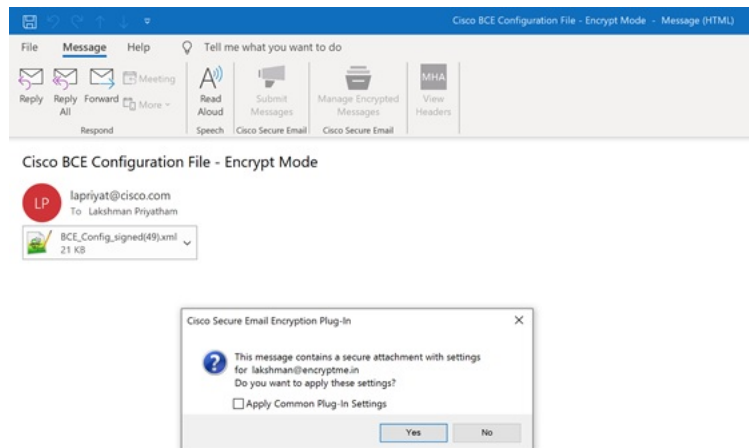


- (注) 通常は、プラグインのインストール時に Java Runtime Environment (JRE) が自動的にインストールされます。ただし、これが実行されない場合は、JREを手動でインストールする必要があります。サポートされているバージョンは、JRE 1.8 または Open JRE 11 です。

Outlook 電子メールアカウントに対して Cisco Secure Email Encryption Plug-in を有効にして設定するには、次の手順を実行します。

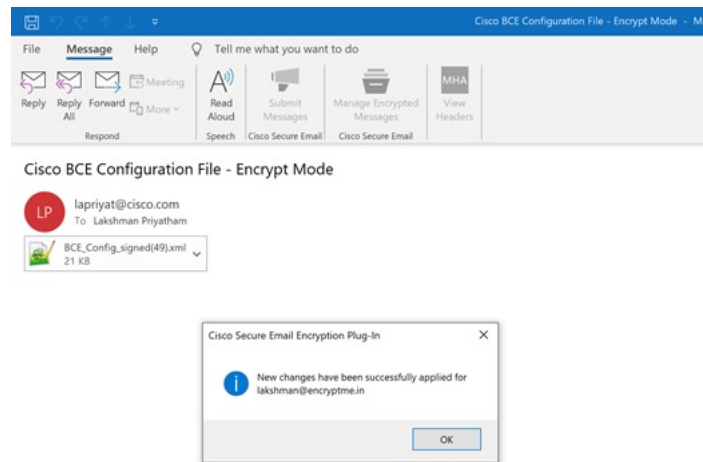
手順

- ステップ 1** 署名された BCE Config ファイルが添付された通知メール メッセージを開きます。設定の適用について確認を求めるメッセージが表示されます。



ステップ 2 [Yes] をクリックして、Cisco Secure Email Encryption Plug-in を設定します。設定が正常に適用されると、メッセージが表示されます。

[Apply Common Plug-in Setting] チェックボックスをオンにすると、プラグインの共通の設定も適用されます。共通のプラグインの設定については、[BCE_Config ファイルを使用した共通オプションの設定 \(7 ページ\)](#) を参照してください。



Flag 暗号化

Flag 暗号化オプションを使用すると、エンドユーザーは暗号化に必要なフラグを設定できます。また、Cisco Secure Email Gateway によって電子メールが暗号化されてから電子メールがネットワークの外部に送信されます。社内ネットワークから外部に発信されるメールに対してスパムやウイルスのスキャンが必要な場合は、Flag 暗号化方式を使用する必要があります。

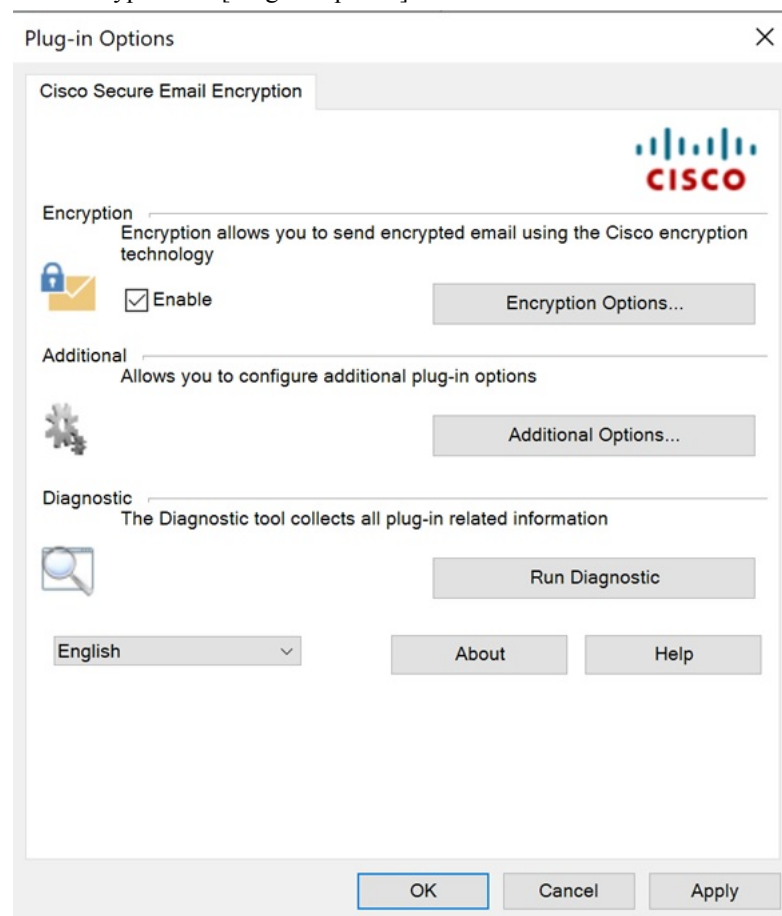
Flag 暗号化の設定は [Cisco Email Security Encryption] ページにあります。Flag 暗号化の設定を変更するには、次の手順を実行します。

- Outlook 2010/2013/2016 では、リボンの [Plug-in Options] ボタンをクリックするか、または [File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Encryption] > [Encryption Options] に移動します。
- Outlook 2007 では、ツールバーの [Plug-in Options] ボタンをクリックするか、または [Tools] > [Options] > [Cisco Email Encryption] > [Encryption Options] に移動します。

暗号化プラグインを有効または無効にするには、[Cisco Secure Email Encryption] タブで [Encryption] フィールドの [Enable] チェックボックスをオンまたはオフにします。

[Enable] をオンにすると、電子メールプログラムからセキュアエンベロープで機密メールを送信できます。

Cisco Secure Email Encryption の [Plug-in Options] ページ :



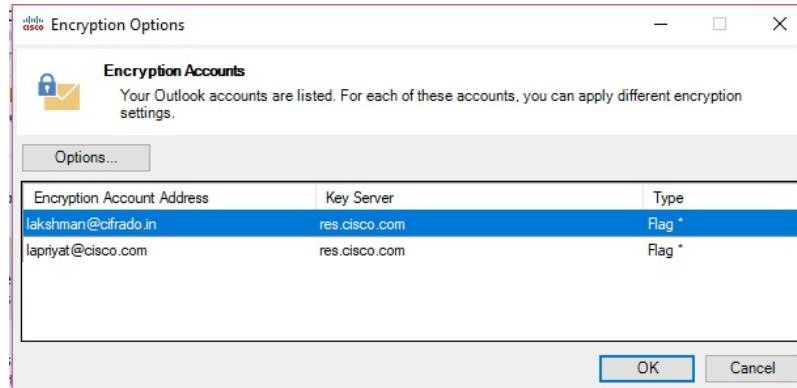
Flag 暗号化のオプション

[Encryption Options] をクリックすると、[Encryption Accounts] ページが表示されます。

Flag 暗号化された電子メールの送信オプション

[Encryption Accounts] ページには、Flag Encryption Plug-in のすべての電子メール ユーザー アカウントが表示されます。各行には、Outlook アカウントの電子メール アドレスと、それに関連付けられているキーサーバーおよび暗号化タイプ（Flag または Encrypt）が示されます。[Options] をクリックするか、アカウントアドレスをダブルクリックすると、[Encryption Options] ページが開きます。

[Encryption Accounts] ページ :



- (注) Outlook の新規アカウントは [Encryption Accounts] リストに自動的に追加されます。Outlook アカウントが削除されると、そのアカウントは [Encryption Accounts] リストから自動的に削除されます。

Flag 暗号化された電子メールの送信オプション

エンドユーザーが送信電子メールを暗号化する場合に、暗号化対象として電子メールにマークを付ける、つまり「フラグを付ける」必要があります。これにより、管理者が作成したフィルタを使って暗号化が必要なメッセージを識別できます。



- (注) 暗号化が必要な電子メールにフラグを設定するこの暗号化方式では、正しく機能するように電子メール フィルタを変更する必要がありますが、この変更は管理者だけが実行できます。

[Encrypt Message] ボタンは電子メールの作成時に使用できます。次のいずれかの方法で電子メールに暗号化のマークを設定できます。

[General] タブ

次の [General] のオプションから選択できます。

[General] のオプション	値
Flag Subject Text	暗号化の電子メールにフラグを設定するように発信電子メールの [Subject] フィールドに追加できるテキスト。[Subject] フィールドに追加するテキストを入力して、電子メールを暗号化する必要があることを示します (デフォルト値は [SEND SECURE])。
Flag X-header name/value	暗号化対象として電子メールにフラグを付ける X ヘッダーを送信電子メールに追加できます。1 つめのフィールドに x ヘッダーを入力します (デフォルト値は <i>x-ironport-encrypt</i> です)。2 つめのフィールドに true または false を入力します。true を入力した場合、指定された x ヘッダーのメッセージが暗号化されます (デフォルト値は true です)。

[Connection] タブ

次の [Connection] のオプションから選択できます。

[Connection] のオプション	値
No proxy	プロキシを使用しない場合に選択します。
Use system proxy settings	デフォルトのシステム プロキシ設定を使用する場合に選択します。
Manual proxy configuration	特定のプロキシ設定を入力する場合に選択します。
Protocol	デフォルトの接続設定を使用しないことを選択した場合、[HTTP]、[SOCKS4]、[SOCKS4a]、[SOCKS5] のいずれかのプロトコルを選択します。
Host	システムまたはプロキシ サーバのホスト名または IP アドレスを指定します。
Port	システムまたはプロキシ サーバーのポートを指定します。
Username	サーバーでユーザー名が必要な場合に、ユーザー名を入力します。

[Connection] のオプション	値
Password	システムまたはプロキシサーバーに対して入力したユーザー名に関連するパスワードを入力します。

[Remember Password] タブ

次の [Remember Password] のオプションから選択します。

パスワードのオプション	値
Never	このオプションを選択すると、電子メールを復号化または暗号化するとき、常に暗号化パスワードが必要になります。
Always	このオプションを選択すると、最初に電子メールを復号化または暗号化するときのみ、暗号化パスワードが必要になります。パスワードはキャッシュされます。
Minutes	暗号化パスワードがキャッシュされるようにするには、このオプションをオンにします。パスワードを思い出すまでの分数を入力するか、矢印を使用して分数を変更します。指定した時間が経過すると、エンドユーザーは、暗号化された電子メールを復号化する際に暗号化パスワードの再入力が必要になります。デフォルトは 1440 分です。

Desktop Encryption

デスクトップ暗号化オプションでは、Outlook 内から電子メールを暗号化し、それをデスクトップから送信できます。

Desktop Encryption 設定は [Cisco Email Security Encryption] ページにあります。Desktop Encryption の設定を変更するには、次の手順を実行します。

- Outlook 2010/2013/2016 では、リボンの [Plug-in Options] ボタンをクリックするか、または [File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Encryption] > [Encryption Options] に移動します。
- Outlook 2007 では、ツールバーの [Plug-in Options] ボタンをクリックするか、または [Tools] > [Options] > [Cisco Email Encryption] > [Encryption Options] に移動します。

エンドユーザーが暗号化プラグインを有効または無効にするには、[Cisco Secure Email Encryption] タブで [Encryption] フィールドの [Enable] チェックボックスをオンまたはオフにします。[Enable]

をオンにすると、電子メール プログラムからセキュア エンベロープで機密メールを送信できます。



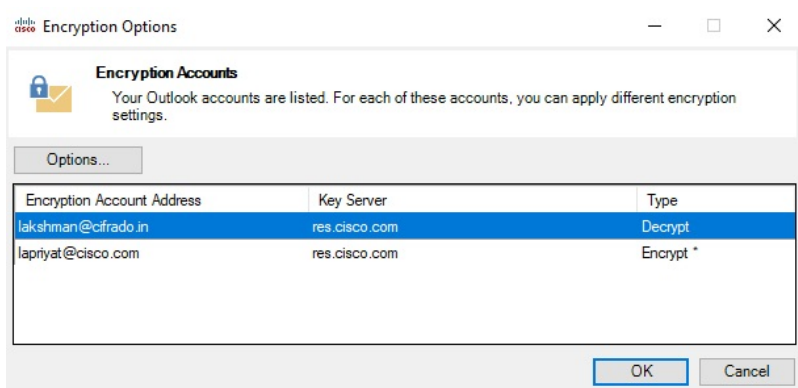
- (注) エンドユーザーは [Cisco Secure Email Encryption] ページから暗号化プラグインを有効化/無効化できますが、暗号化モードに対する変更は、管理者が `BCE_config.xml` ファイルを使って行う必要があります。

デスクトップ暗号化のオプション

[Encryption Options] をクリックすると、[Encryption Accounts] ページが開きます。

[Encryption Accounts] ページには、Flag Encryption Plug-in のすべての電子メール ユーザー アカウントが表示されます。各行には、Outlook アカウントの電子メールアドレスと、それに関連付けられているキーサーバーおよび暗号化タイプ (Flag または Encrypt) が示されます。[Options] をクリックするか、アカウントアドレスをダブルクリックすると、[Encryption Options] ページが開きます。

[Encryption Accounts] ページ :



- (注) Outlook の新規アカウントは [Encryption Accounts] リストに自動的に追加されます。Outlook アカウントが削除されると、そのアカウントは [Encryption Accounts] リストから自動的に削除されます。

[General] タブ



- (注) 次の表に、[General] タブで使用できるすべてのオプションを示します。BCE_config.xml ファイルの設定によっては、表示されない、または使用できないオプションもあります。

次の [General] のオプションから選択します。

[General] のオプション	値
Use as default encryption account	アカウントを、デフォルトの暗号化アカウントとして設定する場合に選択します。
Encrypt by default	すべての送信電子メール メッセージをデフォルトで暗号化する場合に選択します。
Server URL	暗号化サーバの URL を入力します。
Always use message body from key server	プラグインが、各受信者のロケールセットに応じてメッセージ本文に使用する言語を判断できるようにします。このオプションは、同じロケールを使用する受信者に暗号化メッセージを送信する場合に使用します。このオプションをオフにすると、メッセージ本文は常に下のオプションで選択したデフォルトの言語を使用します。
Default language for outgoing messages	異なるロケールを使用する受信者へのメッセージを送信するときに、送信メッセージで使用する言語を指定します（すぐ上のチェックボックスがオンの場合）。 すべての送信メッセージで使用する言語を指定します（すぐ上のチェックボックスはオフになっています）。
Token File Name	トークンは、電子メール クライアントと暗号化サーバー間でデータを暗号化するために使用されるカスタマー固有のキーです。現在、この情報はカスタマー サポートでのみ使用され、変更できません。
Default Expiration (days)	暗号化された電子メールが有効な日数を指定します。有効期間の日数が経過すると、メッセージの有効期限が切れ、それ以降は受信者が開くことができなくなります。
Default read-by (days)	受信者が暗号化されたメッセージを読むことが予想される期間を日数で指定します。指定した期間内にメッセージが読まれなかった場合は、送信者に通知が送られます。
Attachment name	デフォルトのセキュアメッセージ名は <i>securedoc.html</i> です。添付ライフ名は変更でき、セキュアメッセージに指定した新しい名前が反映されます。

[General] のオプション	値
Message Security	<p>暗号化した電子メールのセキュリティを設定します。デフォルト値は <i>BCE_Config.xml</i> ファイルに定義されています。</p> <p>(注) ここで変更したメッセージセキュリティは、作成中のメッセージに対してのみ適用されます。</p> <ul style="list-style-type: none"> • [High (高)]: メッセージに高いセキュリティを指定した場合、暗号化メッセージを復号化するたびに認証用のパスワードが要求されます。 • [Medium (中)]: メッセージに中程度のセキュリティを指定した場合、受信者のパスワードがキャッシュされていれば、メッセージを復号化する際でもパスワードは要求されません。 • [Low (低)]: メッセージに低いセキュリティを指定した場合、メッセージは安全に送信されますが、メッセージを復号化する際でもパスワードが要求されません。
Send return receipt	送信した電子メールを受信者が開封した際に返信確認メッセージを要求する場合に選択します。
Show dialog during message encryption	暗号化するメッセージごとに暗号化オプションダイアログボックスを表示するには、このオプションをオンにします。

[Connection] タブ

次の [Connection] のオプションから選択できます。

[Connection] のオプション	値
No proxy	プロキシを使用しない場合に選択します。
Use system proxy settings	デフォルトのシステム プロキシ設定を使用する場合に選択します。
Manual proxy configuration	特定のプロキシ設定を入力する場合に選択します。

[Connection] のオプション	値
Protocol	デフォルトの接続設定を使用しないことを選択した場合、[HTTP]、[SOCKS4]、[SOCKS4a]、[SOCKS5] のいずれかのプロトコルを選択します。
Host	システムまたはプロキシ サーバのホスト名または IP アドレスを指定します。
Port	システムまたはプロキシ サーバーのポートを指定します。
Username	サーバーでユーザー名が必要な場合に、ユーザー名を入力します。
Password	システムまたはプロキシ サーバーに対して入力したユーザー名に関連するパスワードを入力します。

[Remember Password] タブ

次の [Remember Password] のオプションから選択します。

パスワードのオプション	値
Never	このオプションを選択すると、電子メールを復号化または暗号化するときに、常に暗号化パスワードが必要になります。
Always	このオプションを選択すると、最初に電子メールを復号化または暗号化するときのみ、暗号化パスワードが必要になります。パスワードはキャッシュされます。
Minutes	暗号化パスワードがキャッシュされるようにするには、このオプションをオンにします。パスワードを思い出すまでの分数を入力するか、矢印を使用して分数を変更します。指定した時間が経過すると、エンドユーザーは、暗号化された電子メールを復号化する際に暗号化パスワードの再入力が必要になります。デフォルトは 1440 分です。

[Advanced] タブ



(注) 次の表に、[General] タブで使用できるすべてのオプションを示します。BCE_config.xml ファイルの設定によっては、表示されない、または使用できないオプションもあります。

次の [Advanced] のオプションから選択します。

[Advanced] のオプション	値
Unsecure server URL	メッセージバーのヘルプで使用する、セキュリティで保護されていない URL。このオプションを省略した場合は、外部のセキュア URL (http://res.cisco.com) が使用されます。
Connection timeout	キー サーバへの接続が確立されるまでの待機時間。
Socket timeout	キー サーバーからのデータを待機する時間の長さ。
Display "Open offline" check box	このオプションを選択すると、セキュアメッセージに [Open offline] チェックボックスが表示されます。
Display "Remember envelope key"	このオプションを選択すると、セキュアメッセージに [Remember envelope key] チェックボックスが表示されます。
Display "Enable personal security phrase"	このオプションを選択すると、セキュアメッセージに [Enable personal security phrase] チェックボックスが表示されます。
Add message bar	セキュアメッセージにメッセージバーを追加する場合に選択します。
Show "Reply" button in the message bar	メッセージバーが有効になっている場合、メッセージバーに [Reply] が表示されます。
Show "Forward" button in the message bar	メッセージバーが有効になっている場合、メッセージバーに [Forward] が表示されます。
Show "Reply to All" button in the message bar	メッセージバーが有効になっている場合、メッセージバーに [Reply to All] が表示されます。
Display "Remember me"	このオプションを選択すると、セキュアメッセージに [Remember me] チェックボックスが表示されます。

[Advanced] のオプション	値
Display "Auto open"	このオプションを選択すると、セキュアメッセージに [Auto open] チェックボックスが表示されます。
Open in the same window	セキュアメッセージと同じウィンドウでセキュアメッセージを開く場合に選択します。
Display "Encryption usage reminder"	このオプションを選択すると、ユーザーが暗号化を実行するたびに、ビジネス目的でのみ暗号化を使用するというリマインダが表示されます。

暗号化された電子メールの送信

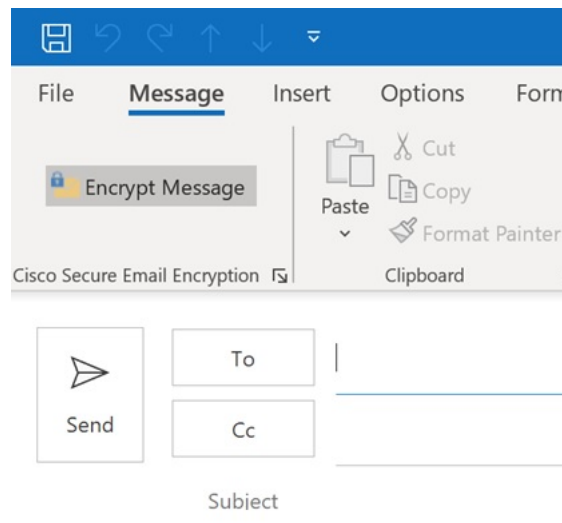


(注) 暗号化電子メールのデフォルトの最大サイズは7MBですが、この値は管理者が *BCE_Config.xml* ファイルを使って変更できます (最大 25 MB)。

エンドユーザーは電子メールの作成時に [Encrypt Message] ボタンをクリックすることで、電子メールを安全に送信することができます。セキュアメッセージを送信する前に、[Encrypt Message] ボタンがオンになっていることを確認してください。

[Encrypt Message] ボタンは電子メールの作成時に使用できます。

次の図に、[Mail Compose] ページの [Encrypt Message] ボタンと [Encryption Mail Options] トグルボタンを示します。

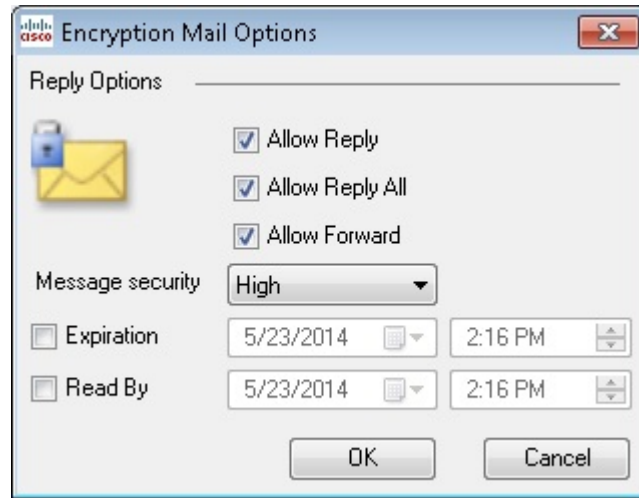


暗号化されたメッセージを送信するには、キーサーバーを選択してパスワードを入力します。

暗号化オプションを設定するには、右下隅の [Cisco Secure Email Encryption] ランチャをクリックして次の [Encryption Mail Options] ページを表示します。



- (注) 次のスクリーンショットと表に [Encryption Mail Options] のオプションのすべてを示します。ただし、表示されるオプションは *BCE_config.xml* ファイルの設定に応じて異なります。



- (注) [Encryption Mail Options] を変更した場合、その変更は作成中の電子メールメッセージにのみ適用されます。

次のメール オプションから選択します。

[Encryption Mail Options]	説明
Allow Reply	このオプションを選択すると、受信者は暗号化電子メールに返信できるようになり、返信の電子メールメッセージが自動的に暗号化されます。
Allow Reply All	このオプションを選択すると、受信者は暗号化電子メールを受信した全員に返信できるようになり、返信の電子メールメッセージが自動的に暗号化されます。
Allow Forward	このオプションを選択すると、受信者は暗号化電子メールを転送できるようになり、転送する電子メールメッセージが自動的に暗号化されます。

[Encryption Mail Options]	説明
<p align="center">Message Security</p>	<p>暗号化した電子メールのセキュリティを設定します。デフォルト値は <i>BCE_Config.xml</i> ファイルに定義されています。</p> <p>(注) ここで変更したメッセージセキュリティは、作成中のメッセージに対してのみ適用されます。</p> <ul style="list-style-type: none"> • [High (高)]: メッセージに高いセキュリティを指定した場合、暗号化メッセージを復号化するたびに認証用のパスワードが要求されます。 • [Medium (中)]: メッセージに中程度のセキュリティを指定した場合、受信者のパスワードがキャッシュされていれば、メッセージを復号化する際でもパスワードは要求されません。 • [Low (低)]: メッセージに低いセキュリティを指定した場合、メッセージは安全に送信されますが、メッセージを復号化する際でもパスワードが要求されません。
<p align="center">Expiration</p>	<p>ドロップダウンから、暗号化されたメールの有効期間 (日時) を指定します。この有効期間が過ぎると、メッセージは期限切れとなり、それ以降は受信者がそのメッセージを開くことはできなくなります。</p>
<p align="center">Read By</p>	<p>ドロップダウンから、受信者が暗号化メッセージを読むと予想される期間 (日時) を指定します。指定した期間内にメッセージが読まれなかった場合は、送信者に通知が送られます。</p>

このオプションが無効になっていない場合は、エンドユーザーが [Send] をクリックすると、[セキュアエンベロープのオプションの設定 \(27 ページ\)](#) に示すような [Secure Envelope Options] ページが開きます。

設定を誤るとエラーが発生することがあります。詳細については、[エラーとトラブルシューティング \(40 ページ\)](#) を参照してください。

返信オプションの伝播

メッセージを復号化すると、[Reply]、[Reply All]、または[Forward] オプションのすべての設定と [Message Sensitivity] オプションのすべての設定が元のメッセージから継承されます。これらは変更できません。次に例を示します。

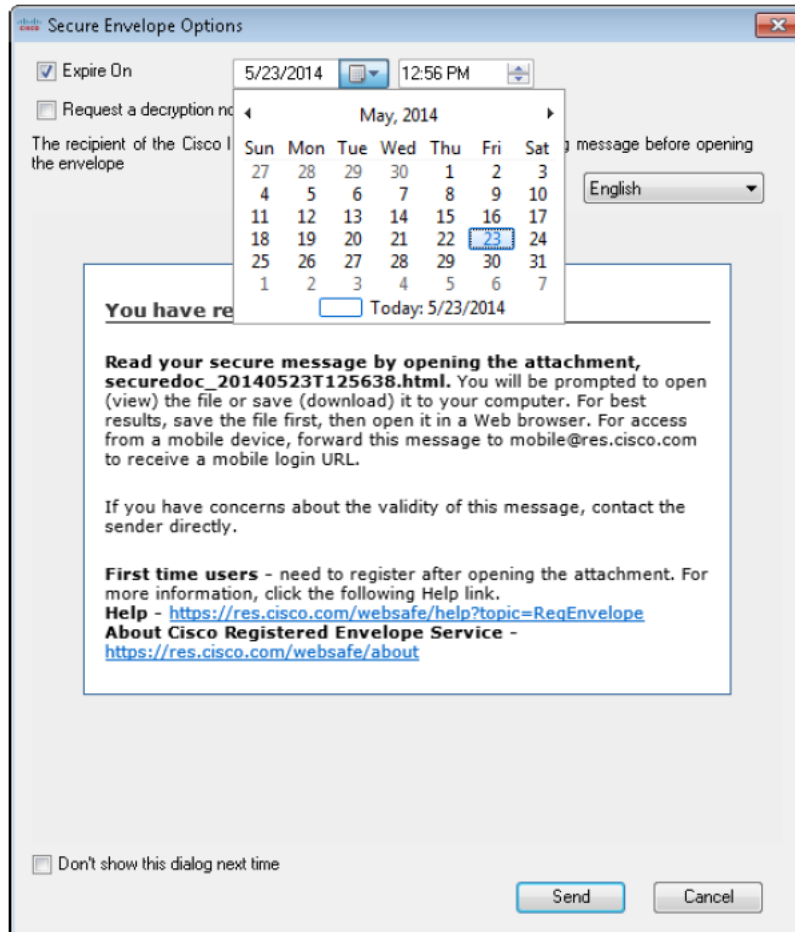
- デフォルトでは、メッセージは返信または転送される際に暗号化されます。
- [Reply]、[Reply All]、または[Forward] オプションを元のメッセージから継承できない場合は、返信メッセージや転送メッセージを送信できず、エンドユーザーが [Send] をクリックするとそのことが通知されます。
- エンドユーザーが [Reply]、[Reply All]、または [Forward] オプションを実行しているときは、元のメッセージに含まれている受信者を削除できません。
- エンドユーザーが [Reply]、[Reply All]、または [Forward] オプションを実行しているときは、元のメッセージに含まれていない受信者を追加できません。
- エンドユーザーが [Reply]、[Reply All]、または [Forward] オプションを実行しているときは、[To]、[Cc]、または[Bcc] フィールド間で受信者を混在させたり、移動することはできません。
- アカウントが [Decrypt Only] または [Flag Encrypt] に設定されている場合は、返信メッセージや転送メッセージを送信できず、エンドユーザーが [Send] をクリックするとそのことが通知されます。
- アカウントの [Message Sensitivity] を [High] に設定すると、[Reply]、[Reply All]、または [Forward] のメッセージの機密性も [High] になります。
- アカウントの [Message Sensitivity] を [Medium] に設定すると、[Reply]、[Reply All]、または [Forward] のメッセージの機密性も [Medium] になります。
- アカウントの [Message Sensitivity] を [Low] に設定すると、[Reply]、[Reply All]、または [Forward] のメッセージの機密性も [Low] になります。
- [Reply]、[Reply All]、または [Forward] のメッセージは [Sent Items] フォルダに保存され、送信者によって復号化できます。
- 署名された BCE Config ファイルが含まれているメッセージを他のエンドユーザーに転送すると、管理者から受け取る場合とは異なり、自動設定が機能せず、エラーが返されません。

セキュアエンベロープのオプションの設定

エンドユーザーは、次のスクリーンショットに示されているように、以下の表に記載されているセキュアエンベロープのオプションを設定できます。



- (注) 設定によっては、画面に言語オプションが表示されないことがあります。また、通知の言語は受信者の設定に応じて選択されます。



セキュアエンベロープのオプション	説明
Expire on	このオプションを有効にする場合に選択します。暗号化電子メールが期限切れになる日時を指定します。その日時を過ぎるとメッセージは期限切れとなり、以降、受信者はそのメッセージを開くことができなくなります。日時は送信者のローカルタイムゾーンに表示されます。
Request a Decryption Notification	送信者がメッセージの復号化通知を要求できるようになります。暗号化されたメッセージが開封されると、送信者に通知が送られます。
Language	通知テキストで使用する言語を選択します。ドロップダウンリストから言語を選択すると、その言語で受信者通知が表示されるようになります。

エンドユーザーのアカウントに Flag 暗号化が設定されている場合は、組織から送信される前に、電子メールに暗号化のフラグが設定されます。エンドユーザーのアカウントにデスクトップ暗号化が設定されている場合、電子メールは、Exchange Server に送信される前に、デスクトップで暗号化されます。

セキュアメッセージの管理

エンドユーザーは次の2つの方法でセキュアメッセージを管理できます。

- [Manage Secure Messages] ダイアログを使用して、選択したメッセージを管理します。このダイアログを使用して、送信した暗号化メールの有効期限をロック、ロック解除、または更新します。
- [メッセージの管理] ダイアログを使って、選択したアカウントから送信されたすべてのメッセージを管理します。このダイアログを使用して特定のメッセージを検索します。

セキュアメッセージを管理するこれらの2つの方法については、次のセクションで説明しています。エンドユーザーはいずれかの方法を使用して、送信した暗号化メールについて以下のことを実行できます。

- **電子メールのロック**。エンドユーザーは、以前に送信した暗号化電子メールをロックできます。また、ロックの理由を設定したり、メッセージがすでにロックされている場合はロックの理由を更新できます。受信者はロックされた電子メールを開くことができなくなります。
- **電子メールのロック解除**。エンドユーザーは、以前に送信した暗号化電子メールのロックを解除できます。これによって、受信者はその電子メールを復号化できるようになります。
- **有効期限の更新**。エンドユーザーは、送信した暗号化電子メールに対して有効期限を設定、更新、クリアすることができます。暗号化された電子メールが期限切れになると、受信者はその電子メールを復号化できなくなります。

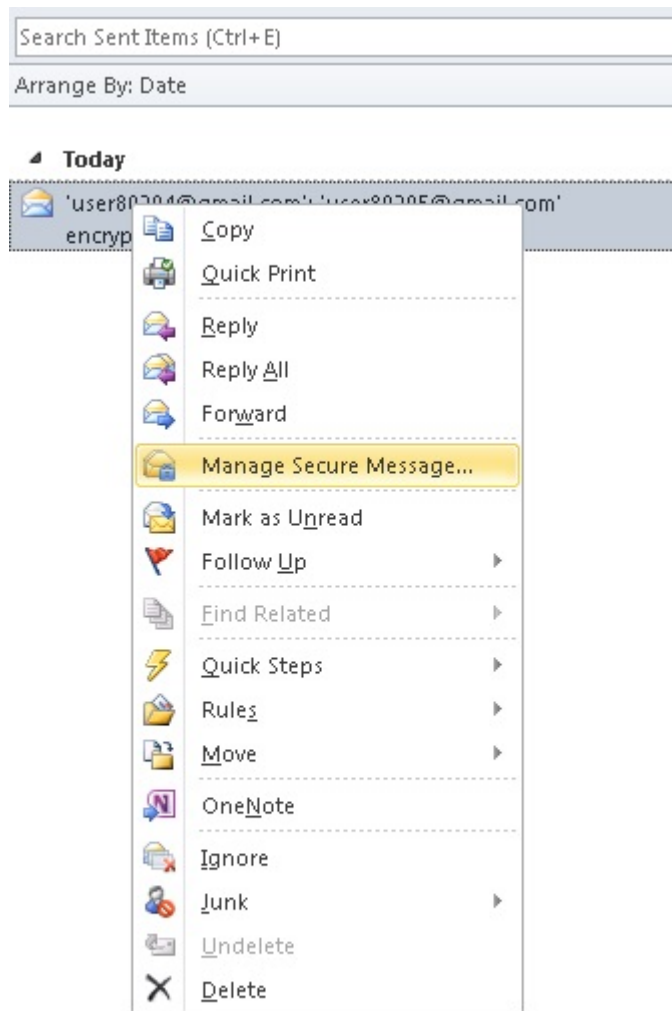
[Manage Secure Messages] ダイアログの使用

手順

ステップ 1 変更する送信済みの暗号化電子メールを選択し、その電子メールを右クリックして [Manage Secure Messages] メニュー オプションを表示します。

(注) また、エンドユーザーは、暗号化された電子メールを復号化するときに [Manage Secure Messages] メニューにアクセスできます。エンドユーザーが変更対象の電子メールの送信者である場合は、ツールバーに [Manage Secure Messages] ボタンが表示されます。ツールバーから [Manage Secure Messages] メニューにアクセスした場合は、同時に1つのメッセージにのみ有効期限の設定を適用できます。

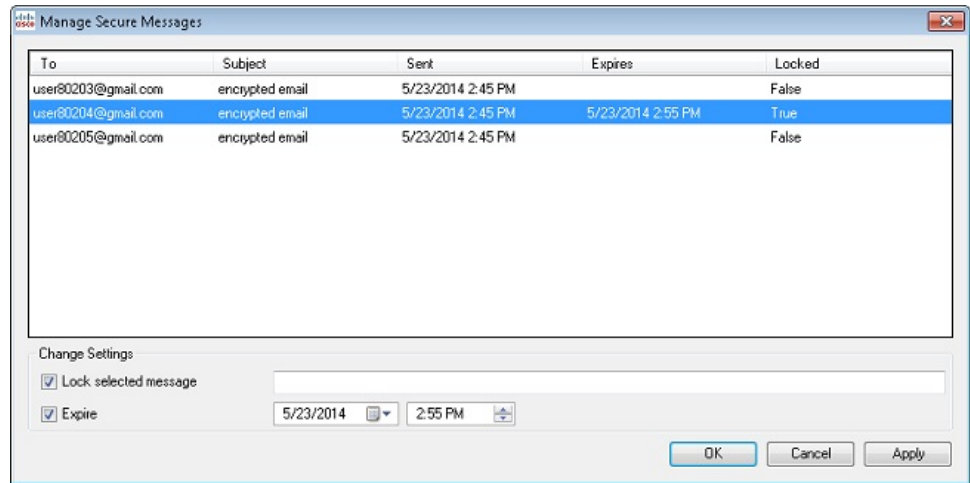
[Manage Secure Messages] メニューのオプション：



ステップ 2 [Manage Secure Messages] を選択します。

パスワードがキャッシュされていない場合は、パスワードの入力が求められます。

[Manage Secure Messages] ページが表示されます。



ステップ 3 受信者ごとにロックまたは有効期限のオプションを設定するには、送信した暗号化電子メールメッセージを1つ以上選択して [Lock] または [Expire] チェックボックスをオンにして、適切な情報を入力します。

(注) ツールバーまたはリボンから [Manage Secure Messages] メニューにアクセスした場合は、次のセクションに記載されているように、有効期限の設定は一度に1つのメッセージにしか適用できません。

[Manage Messages] ダイアログの使用

手順

ステップ 1 リボン (Outlook 2010/13 の場合) またはツールバー (Outlook 2007 の場合) の [Manage Messages] ボタンをクリックします。

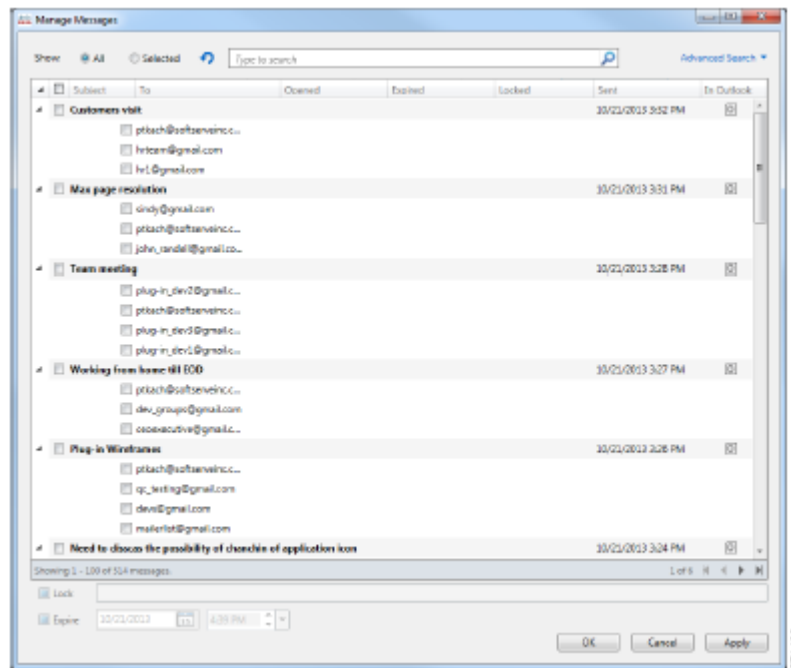
[Manage Messages] ダイアログが開きます。

(注) エンドユーザーはこのインターフェイスを使用して、送信したすべての暗号化メッセージを管理することができます。インターネット接続が遅く、多数の暗号化メッセージがある場合は、ロードのプロセスに数分かかることがあります。

ステップ 2 特定のメッセージを検索するには、[Basic Search] または [Advanced Search] をクリックします。

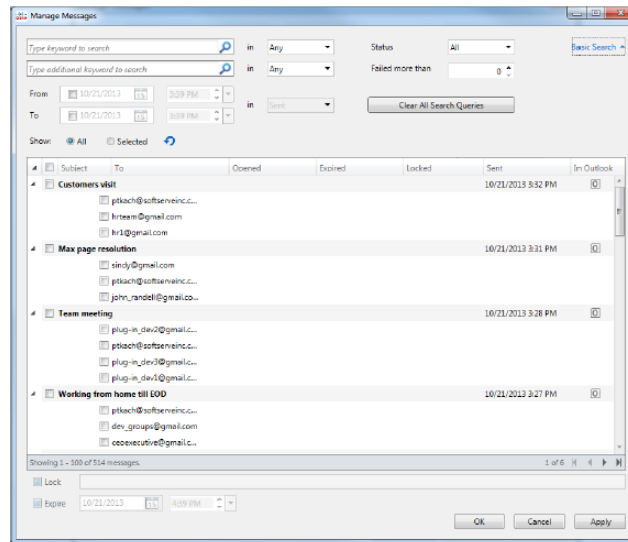
ステップ 3 基本の検索を実行するには、次の画面の [To] フィールドと [Subject] フィールドに検索するキーワードを入力します。

文字列の最大長は 500 です。



ステップ 4 高度な検索を実行するには、次の画面で以下の検索パラメータを 1 つ以上設定します。

- [Keyword 1] : この文字列を使用して、[To] フィールドまたは [Subject] フィールドにキーワードが含まれているメッセージを検索します。キーワードの最大長は 500 文字です。
- [Keyword2] : [Keyword 1] と同じように使用します。両方のキーワードを指定すると、キーワードが 2 つとも含まれているメッセージを照合して検索が実行されます。
- [In] (キーワードの検索用) : [To]、[Subject]、または [Locked Reason] フィールドでキーワードの検索を行うかどうかを指定します。
- [Failed more than] : このオプションを使用すると、失敗した試行回数に基づいて検索が実行されます。結果として表示されるメッセージには、指定した値を超えた、メールが失敗した試行回数が含まれます。最大値は 10 です。
- [Status] : このオプションを使用すると、[All]、[Unopened]、[Opened]、[Locked]、および [Expired] のいずれかのステータスの設定に基づいて検索を実行します。
- [From/To] : このオプションを使用すると、日付と時間の間隔に基づいて検索が実行されます。[From] の日付のみを設定した場合は、選択した日付より後に送信されたメッセージに対して検索が行われます。[To] の日付のみを設定した場合は、選択した日付より前に送信されたメッセージに対して検索が行われます。両方の日付を設定した場合は、選択した 2 つの日付の間に送信されたメッセージに対して検索が行われます。日付を設定するには、ドロップダウンのカレンダーを使用するか、または手動で日付を入力します。デフォルトの日付は現在の日時ですが、日付による検索はデフォルトで無効になっています。
- [In] (日付の検索用) : 日付関係の検索の基準を指定します。使用できるオプションは [Sent]、[Opened]、および [Expired] です。



ステップ5 [OK] をクリックします。

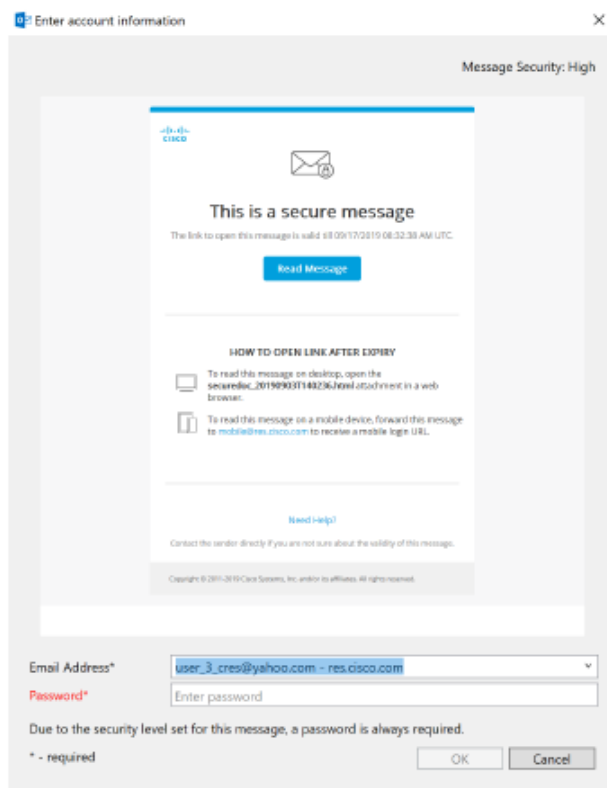
安全な電子メールの受信と返信

デスクトップ暗号化プラグインは安全な電子メールを自動的に検出し、Outlook 内でそれらの復号化を試みます。エンドユーザーが暗号化されたメッセージを受信した場合は、通常、エンベロープを開封するために暗号化パスワードを入力する必要があります。セキュアメッセージには、[High]、[Medium]、または [Low] のメッセージセキュリティを設定できます。

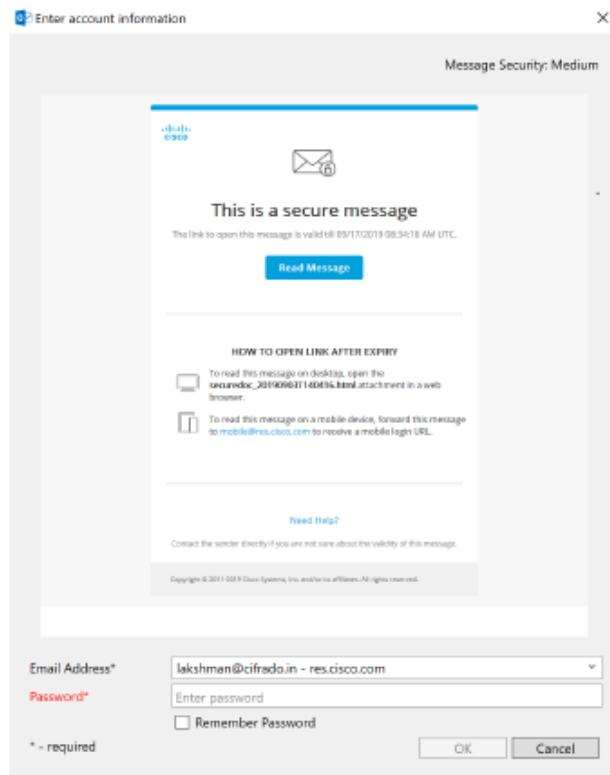


- (注) パスワードで保護されたセキュリティメッセージを受信した場合、エンドユーザーは、そのメッセージを開封するために、Cisco Secure Email Encryption Service にユーザーアカウントを登録して設定しなければならないことがあります。サービスに登録すると、アカウントパスワードを使用して、受信するすべての登録済みエンベロープを開封できます。詳細については、[安全な返信/すべてに返信/転送 \(37 ページ\)](#) を参照してください。

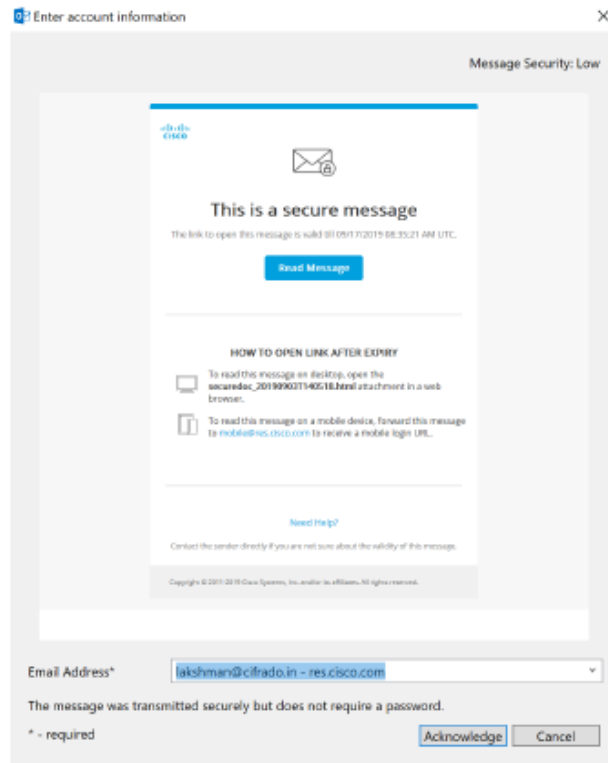
[Message Encryption High] ページ :



[Message Encryption Medium] ページ



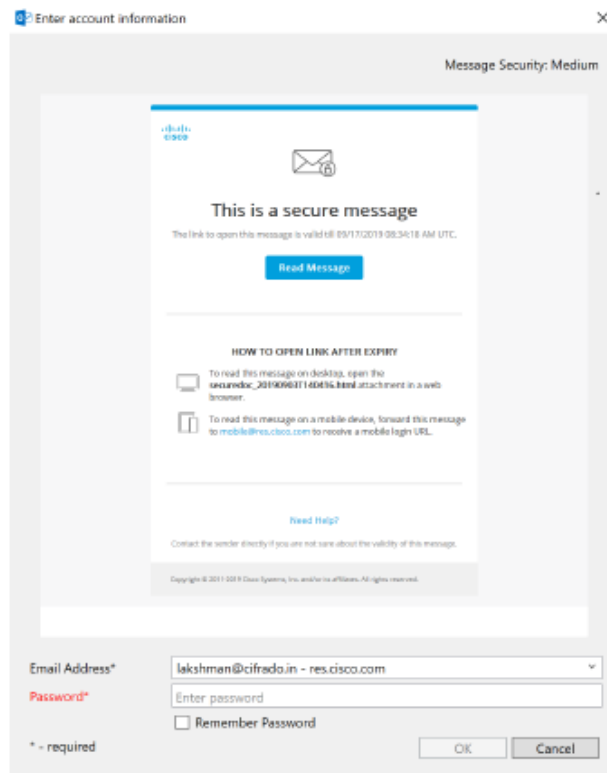
[Message Encryption Low] ページ :



次の表は、メッセージセキュリティのオプションを示しています。

メッセージセキュリティのオプション	説明
High	メッセージに高度のセキュリティを指定すると、暗号化されたメッセージを復号化するたびに認証用のパスワードが要求されます。
Medium	メッセージに中程度のセキュリティを指定すると、受信者のパスワードがキャッシュされている場合は、そのメッセージを復号化するときにパスワードは要求されません。
Low	メッセージに低いセキュリティを指定した場合、送信は安全に行われますが、暗号化されたメッセージを復号化するときにパスワードが要求されません。

エンドユーザーがロックされた（または期限切れの）セキュアメッセージを受信すると、そのことを通知するメッセージが [Message Security] ページに赤い文字で表示されます。



安全な返信/すべてに返信/転送

Desktop Encryption または Decrypt Only モードを使用している場合に、暗号化されたメールに返信したり、転送したりすると、返信はデフォルトで自動的に暗号化されます。Flag 暗号化を使用している場合は、Cisco Secure Email Gateway によって応答メッセージが暗号化されます。セキュアメッセージの設定は、ユーザーが次のアクションを実行できるかどうかによって判断されます。

- 安全な返信
- 全員への安全な返信
- 安全な転送

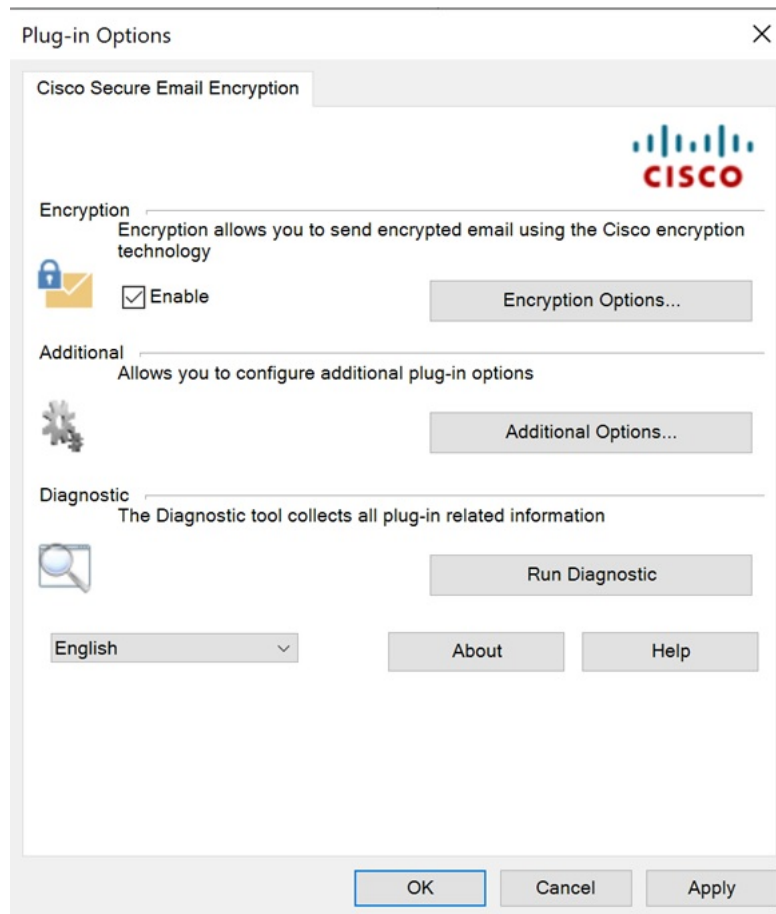
追加設定の変更

ログファイルには、すべての発生したアクションが記録されリスト化されています。

追加のオプションは [Cisco Secure Email Encryption] ページにあります。追加のオプションを変更するには、次の手順を実行します。

- Outlook 2010/2013/2016 では、リボンの [Plug-in Options] ボタンをクリックするか、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Encryption] > [Additional Options] を選択します。
- Outlook 2007 では、ツールバーの [Plug-in Options] ボタンをクリックするか、[Tools] > [Options] > [Cisco Email Encryption] > [Additional Options] を選択します。

Cisco Secure Email Encryption の [Plug-in Options] ページ :



[Encryption Additional Options] ページでは、次のタイプのオプションを設定することができます。これは以降のセクションで説明しています。

- Logging
- Sending Usage Data
- Privacy

[Logging] タブ

エンドユーザーは [Logging] タブで次のオプションを設定できます。

オプション	説明
Enable Logging	Cisco Secure Email Encryption Plug-in のロギングを有効にする場合に選択します。
Log file name	ログ ファイルの名前を指定します。このファイルは %ALLUSERSPROFILE%\Cisco\Cisco Secure Email Encryption Plug-in\ <username> td="" に保存されます。ログ="" ファイル名の最後には、.log="" 拡張子を付ける必要があります。<=""> </username>>
Log level	次のいずれかを選択します。 <ul style="list-style-type: none"> • [Normal] : このオプションはデフォルトで有効になっています。標準ログには致命的なエラー、回復可能なエラー、警告が含まれます。 • [Extended] : ロギングを拡張すると、標準のロギングメッセージに加えて、役立つ情報とデバッグロギングメッセージも有効になります。 <p>特定の状況に必要なトラブルシューティングのレベルに基づいてログ レベルを変更できます。たとえば、Cisco Secure Email Encryption Plug-in で問題が発生した場合、ロギングレベルが [Extended] に設定されていると、開発者に対して可能な限りの情報を提供し、問題の再現と診断に役立ちます。</p>

[Sending Usage Data] タブ

エンドユーザは [使用データの送信 (Sending Usage Data)] タブで次のオプションを設定できます。

オプション	説明
Send anonymous usage data to Cisco	Cisco Secure Email Encryption Plug-in で、製品の改善に使用するためのデータを収集することができます。次の 2 つのタイプの情報が収集され、分析のために Cisco サーバーに保存されます。 <ul style="list-style-type: none"> • プラグインを実行しているマシンに関する一般情報 • アカウント固有の情報

[Privacy] タブ

エンドユーザーは [プライバシー (Privacy)] タブで次のオプションを設定できます。

オプション	説明
Resets Identifier	使用状況レポートの関連付けに使用する ID をリセットします。
Clear All Passwords	すべてのアカウントのキャッシュされているすべてのパスワードをクリアします。

エラーとトラブルシューティング

この項では、Cisco Secure Email Encryption Plug-in for Outlook の使用中に発生する可能性がある一般的なエラーと、それらを解決するためのトラブルシューティングを説明します。



- (注) 同じエラーメッセージを複数回受け取り、そのエラーによって Cisco Secure Email Encryption Plug-in が機能しなくなった場合、エンドユーザーは修復プロセスを実行できます。[Cisco Secure Email Encryption Plug-in for Outlook ファイルの修復 \(43 ページ\)](#) を参照してください。修復プロセスを実行しても同じエラーが発生する場合は、手順に従って診断ツールを使用し、シスコにフィードバックしてください。[Cisco Secure Email Encryption 診断ツールの実行 \(44 ページ\)](#) を参照してください。

Outlook 起動エラー

コンフィギュレーション ファイルの初期化中に発生するエラー

Outlook の起動時に次のメッセージが表示されることがあります。

- *An error occurred during <file_name> configuration file initialization. Some settings have been set to the default values.*
- *Config validation for account <account_address> has failed. Please set the correct configuration values or contact your administrator.*

これらのエラーメッセージは、一部の設定値が無効な場合や、%ALLUSERSPROFILE%\Cisco\Cisco Email Encryption Plug-In\

解決策

Cisco Secure Email Encryption Plug-in は、破損した構成ファイルに含まれている一部の暗号化オプションのデフォルト値を復元しません。代わりに、一部の暗号化機能をオフにします。エ

ラーメッセージが繰り返し表示される場合は、修復プロセスを実行してコンフィギュレーションファイルを修正してください。[Cisco Secure Email Encryption Plug-in for Outlook ファイルの修復 \(43 ページ\)](#) を参照してください。

コンフィギュレーションファイルが見つからない

Outlook の起動時に次のエラーメッセージが表示されることがあります。

- `<file_name> configuration file was not found. Settings have been set to the default values.`

解決策

Cisco Secure Email Encryption Plug-in は、破損した構成ファイルに含まれている一部の暗号化オプションのデフォルト値を復元しません。代わりに、暗号化モードを設定します。エラーメッセージが繰り返し表示される場合は、修復プロセスを実行してコンフィギュレーションファイルを修正してください。[Cisco Secure Email Encryption Plug-in for Outlook ファイルの修復 \(43 ページ\)](#) を参照してください。

復号化および暗号化に関するエラー

オプションが無効にしていない場合は、[Send] をクリックすると [Secure Message Options] ページが表示されます。電子メールアカウントで次のようなステータスメッセージを受信することがあります。

暗号化オプションが無効になっている場合

発生した接続の問題が修正されも [Encryption Options] が無効になっている場合は、Outlook を再起動してください。Outlook を再起動しても解決しない場合は、管理者に問い合わせてください。

アカウントがロックされている場合

- *Your account has been locked. Please contact your account administrator for more information.*

解決策

システム管理者に電子メールアカウントのロック解除を依頼してください。

アカウントがブロックされている場合

- *Your account has been blocked and you must reset your password. Please use the forgot password link to reactivate your account.* [パスワードを忘れた場合](#)

解決策

パスワードリンクをクリックして、パスワードセキュリティの確認用の質問に正しく回答し、パスワードをリセットしてください。

アカウントが一時停止された場合

- *You have no attempts remaining. Your account is locked for the next 15 minutes.*

解決策

後で <https://res.cisco.com/websafe/> にログインを試みるか、サポート (<https://res.cisco.com/websafe/help?topic=ContactSupport>) に連絡してサポートを受けることができます。

受信者が未設定

送信する電子メールに受信者が記入されていない場合、次のメッセージを受け取ることがあります。

- *An error occurred during encryption: no recipients specified.*

復号化中にエラーが発生

メッセージの復号化中に予期しないエラーが発生しました。たとえば、SDKによって不明なエラーコードを返されたり、プラグインによって例外が報告されます。

- *An error occurred during decryption.*

解決策

診断ツールを実行して、サポートチームに診断レポートを送信してください。 [Cisco Secure Email Encryption 診断ツールの実行 \(44 ページ\)](#) を参照してください。

暗号化中にエラーが発生

メッセージの暗号化中に予期しないエラーが発生しました。たとえば、SDKによって不明なエラーコードを返されたり、プラグインによって例外が報告されます。

- *An error occurred during encryption.*

解決策

診断ツールを実行して、サポートチームに診断レポートを送信してください。 [Cisco Secure Email Encryption 診断ツールの実行 \(44 ページ\)](#) を参照してください。

上限を超過

暗号化電子メールのデフォルトの最大サイズは7MBですが、この値は管理者がBCE_Config.xml ファイルを使って変更できます (最大25MB)。暗号化電子メールが最大値を超えている場合は、次のいずれかのメッセージを受け取ります。

- *This message exceeds the allowable limit and cannot be decrypted.*
- *This message exceeds the allowable limit and cannot be encrypted.*

- *An error occurred during encryption: an invalid attachment found.*
- *Failed to report this message. This message is too large.*
- *Failed to report {0} messages. {0} messages are too large.*



(注) 「Failed to report ...」で始まる最後の2つのメッセージは、現在は英語のみです。

Cisco Secure Email Encryption Plug-in for Outlook ファイルの修復

Cisco Secure Email Encryption Plug-in を修復するには、次の手順を実行します。

手順

ステップ 1 Outlook が終了していることを確認します。

ステップ 2 [Control Panel] > [Add or Remove Programs] を選択します。

ステップ 3 プログラムの一覧で [Cisco Secure Email Encryption Plug-in] を見つけて、[Uninstall/Change] をクリックします。

ステップ 4 [Repair] をクリックします。インストーラの修復プロセスが実行されます。

(注) 暗号化の設定は復元したり修正したりできません。暗号化の設定は、管理者のみが *BCE_Config.xml* ファイルを使って送信できます。

ステップ 5 エラーの原因になったアクションを実行します。修復プロセスの実行後も同じエラーが発生する場合、診断ツールを使用してシスコにフィードバックする手順を実行してください。[Cisco Secure Email Encryption 診断ツールの実行 \(44 ページ\)](#) を参照してください。

診断ツールを使用したトラブルシューティング

Cisco Secure Email Encryption Plug-in には、問題のトラブルシューティング時にシスコのサポートを支援する診断ツールが用意されています。診断ツールを使ってプラグインツールから重要なデータを収集し、それらをシスコサポートに送ると問題の解決に役立ちます。

エラーが発生した場合や修復手順では解決できない Cisco Secure Email Encryption Plug-in に関する問題が発生した場合、エンドユーザーは診断ツールを使用できます。また、診断ツールを使用すると、不具合の報告時にシスコのエンジニアと重要情報を共有することもできます。

[Cisco Secure Email Encryption Plug-in for Outlook ファイルの修復 \(43 ページ\)](#) または [Cisco Secure Email Encryption 診断ツールの実行 \(44 ページ\)](#) を参照してください。



(注) エラーが発生した場合は、[エラーとトラブルシューティング \(40 ページ\)](#) のトラブルシューティングのヒントを参照してください。

Cisco Secure Email Encryption 診断ツールにより収集されるデータ

診断ツールは、ご使用のコンピュータから次の情報を収集します。

- 一部の COM コンポーネントに関する登録情報
- 環境変数
- Cisco Secure Email Encryption Plug-in 出力ファイル
- Windows および Outlook に関する情報
- システム ユーザ名および PC 名
- 他の Outlook プラグインに関する情報
- Outlook に関連する Windows イベント ログのエントリ

Cisco Secure Email Encryption 診断ツールの実行

Cisco Email Encryption 診断ツールは、次のいずれかの場所から実行できます。

- **Cisco Secure Email Encryption** の **[Options]** タブから。通常は、Cisco Secure Email Encryption の **[Options]** タブから診断ツールを実行します。
- 「Program Files\Cisco Email Encryption Plug-in」フォルダ（通常は C:\Program Files\Cisco\Cisco Email Encryption Plug-in）から。これは、Cisco Email Encryption Plug-in がインストールされているフォルダです。
- [Start] メニュー > [All Programs] > [Cisco Email Encryption Plug-in] > [Cisco Email Encryption Plug-in Diagnostic] から。

Outlook の [Options] ページからの診断ツールの実行

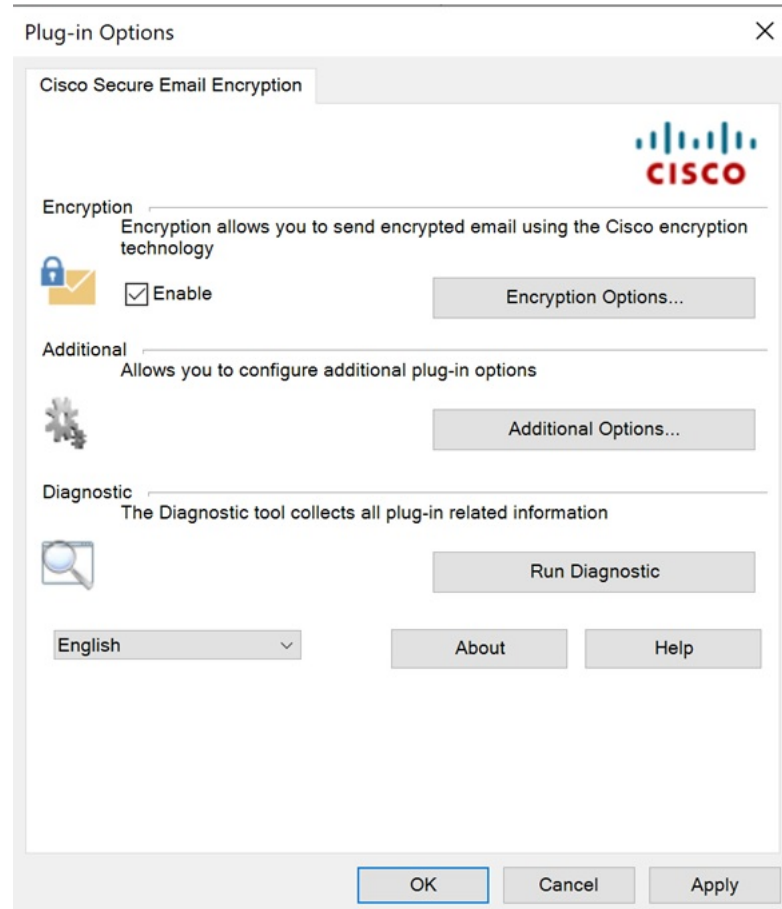
手順

ステップ 1 診断ツールを実行するには、次のように移動します。

- Outlook 2010/2013/2016 では、リボンの **[Plug-in Options]** ボタンをクリックするか、または **[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Encryption] > [Run Diagnostic]** に移動します。

- Outlook 2007 ではツールバーの [Plug-in Options] ボタンをクリックするか、[Tools] > [Options] > [Cisco Email Security Encryption] > [Run Diagnostic] に移動します。

Cisco Secure Email Encryption の [Plug-in Options] ページ :



ステップ 2 診断ツールがデータを収集するまで数秒間待ちます。診断ツールがデータを収集し終わったら、データが正常に収集されたことを示すメッセージが表示されます。

診断ツールにより、*CiscoDiagnosticReport.zip* ファイルが生成され、現在のユーザーの **My Documents** フォルダに保存されます。そのファイルはエンドユーザーがシステム管理者に送信するか、管理者がシスコサポートの担当者に送信できます。レポートを表示するには、*CiscoDiagnosticsReport.zip* ファイルをダブルクリックします。

Program Files からの診断ツールの実行

次の 2 種類の方法で Program files から診断ツールを実行できます。

- [Start] > [Programs] > [Cisco Email Encryption Plug-in] > [Cisco Email Encryption Plug-in Diagnostic] から診断ツールを実行します。

または

- Cisco Secure Email Encryption Plug-in がインストールされているフォルダ（通常は C:\Program Files\Cisco\Cisco Email Encryption Plug-in）に移動し、
Cisco.EmailEncryption.Framework.Diagnostic.exe ファイルをダブルクリックします。

シスコの診断ツールの一般的なエラーのトラブルシューティング

適切なデバッグを行うには、すべての診断ログを拡張モードにする必要があります。

実行中の診断ツールでログ収集が完了したら、次の手順を実行します。

1. *CiscoEncryptionDiagnosticReport\Outlook\UsersAppDataFiles\CiscoEmailEncryption.log* に移動します。
2. ログファイルを開き、次のいずれかの問題が存在するかどうかを確認します。
 - [問題：TLS 接続をネゴシエートできません。（46 ページ）](#)
 - [問題：DNS 名を解決できません。（46 ページ）](#)
 - [問題：HTTP 要求を送信できません。（47 ページ）](#)
 - [問題：Web プロキシサーバーからの応答が無効です。「HTTP/1.0 407 プロキシ認証が必要です」（47 ページ）](#)
 - [問題：クライアントマシンで Java ランタイム環境が見つかりません。（47 ページ）](#)

問題：TLS 接続をネゴシエートできません。

障害：プラグインが Encryption Service サーバー（res.cisco.com）に接続できず、TLS 接続をネゴシエートします。

解決策：プラグインがインストールされているクライアントマシンに Encryption Service サーバー（res.cisco.com）を接続していることを確認します。Encryption Service サーバーとクライアントマシンの間のネットワークでファイアウォールを実行している場合は、次のポートを開く必要があります。

- res.cisco.com（デフォルト（復号）、暗号化、およびフラグモードに使用されます）。
- verify.res.cisco.com（BCE Config 署名中に使用されます）。
- updates.res.cisco.com（Microsoft Outlook の [Plug-in] オプションで [Check for Updates] オプションをクリックすると使用されます）。

問題：DNS 名を解決できません。

障害：プラグインが Encryption Service サーバー（res.cisco.com）に接続できず、DNS 名を解決できません。

解決策：プラグインがインストールされているクライアントマシンに適切なインターネット接続があることを確認します。

問題：HTTP要求を送信できません。

障害：プラグインが Encryption Service サーバー（res.cisco.com）に HTTP 要求を送信できません。

解決策：プラグインがインストールされているクライアントマシンに Encryption Service サーバー（res.cisco.com）を接続していることを確認します。Encryption Service サーバーとクライアントマシンの間のネットワークでファイアウォールを実行している場合は、次のポートを開く必要があります。

- res.cisco.com（デフォルト（復号）、暗号化、およびフラグモードに使用されます）。
- verify.res.cisco.com（BCE Config 署名中に使用されます）。
- updates.res.cisco.com（Microsoft Outlook の [Plug-in] オプションで [Check for Updates] オプションをクリックすると使用されます）。

問題：Web プロキシサーバーからの応答が無効です。「HTTP/1.0 407 プロキシ認証が必要です」

障害：次のいずれかの理由により、プラグインがプロキシサーバーを使用して Encryption Service アプリケーションに接続できません。

- プロキシサーバー認証の詳細（ユーザー名とパスワード）がインストール時に提供されません。
- プロキシサーバーの詳細が無効です。

解決策：プラグインのインストール時に、BCE 構成ファイルで提供されるプロキシサーバーの詳細を確認する必要があります。

問題：クライアントマシンで Java ランタイム環境が見つかりません。

障害：プラグインを含むクライアントマシンに Java ランタイム環境がインストールされていません。

解決策：Java ランタイム環境がクライアントマシンにインストールされていることを確認します。この環境にプラグインが含まれています。

エンベロープでの JavaScript の無効化

受信電子メールがエンベロープで JavaScript を使用している場合、エラーが生じる原因となったり、エンベロープを開けなくなったりする可能性があります。これらの問題を回避するには、次の手順を実行し、生成されたエンベロープで JavaScript を無効にします。

手順

- ステップ 1** キー サーバーから BCE Configuration ファイルのテンプレートをダウンロードします。
- キーサーバーに管理者としてログインし、[Accounts] > [Manage Accounts] > [BCE Config] > [Download Template] を選択します。
- ステップ 2** BCE Configuration ファイルを編集し、<encryption> セクションのいずれかの場所に <usescript>false<usescript> を追加するか、<usescript> タグがすでに存在している場合は値を false に設定します。
- ステップ 3** BCE Configuration ファイルを保存して、キー サーバー上でファイルに署名します。
- ステップ 4** 署名した BCE Configuration ファイルをユーザーに送信します。
-

Cisco Secure Email Encryption Plug-in のアンインストール

Cisco Secure Email Encryption Plug-in をアンインストールするには、[Control Panel] > [Add/Remove Program] オプションを使用するか、または `setup.exe` プログラムを実行します。

アンインストールすると、次の項目が削除されます。

- プラグインによって作成されたすべてのレジストリ エントリ
- [プログラムの追加と削除 (Add/Remove Program)] に一覧表示されているプラグインのエントリ
- プラグインに関連するファイルの一部。すべてのファイルが削除されるわけではないので注意してください。
- プラグイン ツールバー (Outlook から削除)



- (注) プラグインをアンインストールしても Outlook のパフォーマンスには影響しません。アンインストールするときは Outlook を終了しておいてください。
-

Cisco Secure Email Encryption Plug-in for Outlook をアンインストールするには、次の手順を実行します。

Encryption Plug-in for Outlook のアンインストールに使用できる方法には次の 2 つがあります。

手順

- ステップ 1** [Start] > [Control Panel] > [Add/Remove Programs] をクリックします。

ステップ 2 [Cisco Secure Email Encryption Plug In] > を選択し、[Uninstall/Change] > [Next] > [Remove] をクリックします。

もう 1 つのアンインストール方法 :

- プラグインのセットアップファイル (プラグインのインストールに使用したファイル) をダブルクリックし、[Remove] オプションを選択して Cisco Secure Email Encryption Plug-in をアンインストールします。
-

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。