Cisco Secure Email Encryption Plug-in の展開

この章は、次の項で構成されています。

暗号化プラグイン

暗号化プラグインをインストールすると、電子メール メッセージのメニュー バーに [Encrypt Message] ボタンが表示されるので、送信者は、組織外部に送信する前に、暗号化して保護する必要があるメッセージを簡単にマークできます。

2 種類の暗号化（Flag 暗号化とデスクトップ暗号化）を使用できます。Flag 暗号化オプションを使用すると、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。デスクトップ暗号化では、シスコの暗号化テクノロジーを使用して電子メールプログラム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電子メールプログラムによりデスクトップから送信されます。デスクトップ暗号化は、組織内で送信するメールを暗号化する場合に使用できます。

暗号化プラグインは、機能している設定済みの Cisco Secure Email Gateway（ネットワーク内に存在している場合）と連動するように設計されています。暗号化プラグインに使用するコンフィギュレーションは、これらのアプライアンスの設定に合わせて設定する必要があります。これらのアプライアンスに同じ設定を使用しないと、暗号化メッセージを送信するときに問題が生じる可能性があります。

（注） 暗号化プラグインでは、Cisco Secure Email Gateway が存在し、正しく設定されているか、または Cisco Secure Email Encryption Service アカウントが必要です。

Cisco Secure Email Encryption Plug-in のインストール

ユーザーグループ向けに Cisco Secure Email Encryption Plug-in をインストールする場合、サイレントインストールを実行できます。サイレント インストールでは、エンド ユーザーに入力を求めることなくインストールを実行できます。サイレントインストールの詳細については、一括インストールの実行を参照してください。

（注） Cisco Secure Email Encryption Plug-in 7.x と Cisco Secure Email Encryption Plug-in 1.2 を一緒にインストールしないでください。レポート機能が必要な場合は、Cisco Secure Email Encryption Plug-in 1.x と Cisco Secure Email Reporting Plug-in 1.x の両方をインストールします。

コンフィギュレーション モード

Cisco Secure Email Encryption Plug-in は、3 種類のコンフィギュレーション モードで展開されます。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。

他のコンフィギュレーションモードを有効にするには、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 Outlook 電子メール アカウントを設定します。管理者は、エンド ユーザーの電子メール アカウントに BCE Config 添付ファイル（デフォルト名は *BCE_Config_signed.xml*）を送信します。エンド ユーザーはこのファイルを *securedoc.html* ファイルとして受信します。エンド ユーザーが *securedoc.html* 添付ファイルをクリックすると、メッセージに添付されている設定情報が Outlook アプリケーションによって検出され、更新済みの設定が適用されます。

（注） デフォルトのセキュアメッセージ名は *securedoc.html* です。添付ファイル名の値は管理者が変更でき、指定された新しい名前がメッセージに反映されます。

3 つのコンフィギュレーション モードは次のとおりです。

- **Decrypt Only**：受信した安全な電子メール メッセージを復号化できます。
- **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。

次の表は、各コンフィギュレーション モードでサポートされる機能を示しています。

機能	Decrypt Only	Decrypt and Flag	Decrypt and Encrypt
暗号化したメッセージを送信			X
メッセージに暗号化フラグを設定		X	
暗号化された電子メールを開封	X	X	X
返信/すべてに返信/転送	X	X	X
電子メールのロックおよびロック解除	X	X	X
電子メールの有効期限	X	X	X
電子メールの診断	X	X	X
開封確認			X
セキュアメッセージの設定			X
設定	X	X	X

暗号化サービスキーサーバーを使用した Cisco Secure Email Encryption Plug-in の展開

Cisco Secure Email Encryption Service のキーサーバーで直接使用できるように、次の手順を実行して Cisco Secure Email Encryption Plug を展開します。

手順

ステップ 1 Encryption Service アカウント https://res.cisco.com/admin にログインし、[Accounts] タブに移動します。

ステップ 2 Encryption Plug-in を有効にするアカウントを選択します。次に、[BCE Config] タブに移動します。

ステップ 3 設定テンプレートで使用するトークンを選択します。

- [CRES]：キー サーバーが Encryption Service の場合に選択します。

ステップ 4 [Download Template] をクリックして、編集するテンプレート ファイルをダウンロードします。ファイル名は *BCE_Config.xml* です。

ステップ 5 コンフィギュレーション ファイルを編集します。

BCE_Config.xml ファイルには、特定の環境に合わせて編集する必要があるフィールドの詳細が含まれています。テキストエディタでファイルを開き、コメントに記載されている手順に従って必要な変更を行います。

（注） ローカリゼーションが目的の場合は、既存のメッセージセキュリティ ラベル（Low、Medium、High）を変更しないでください。

ステップ 6 [Browse] をクリックして、編集した *BCE_Config.xml* ファイルを探し、ファイルが見つかったら [Upload and Sign] をクリックします。

コンフィギュレーション ファイルに署名すると、その署名したバージョンが *BCE_Config_signed.xml* としてダウンロードされます。このファイルをローカル マシンに保存します。

ステップ 7 同時に多数のエンド ユーザーにコンフィギュレーション ファイルを展開するには、[Distribute Signed Configuration to Bulk List] オプションを使用します。次の手順を実行します。

1. ステップ 6 で作成した BCE 構成ファイルを参照します。
2. エンド ユーザーの電子メール アドレスが含まれているカンマ区切り形式のファイルの場所を参照します。
3. 必要に応じて電子メールの件名を変更します。
4. [Distribute Config] をクリックします。署名付き BCE Config を使用して一括インストールを実行するには、「BCE_Config.xml ファイルによる一括インストールBCE_Config.xml ファイルを使用した一括インストール」の項を参照してください。

（注） XML 構成ファイルを別のエンド ユーザーに転送した場合は、管理者から受け取った場合とは異なり、自動設定が機能せず、エラーが表示されます。Cisco Secure Email Gateway または暗号化サービスによって暗号化された電子メールを介して、すべてのエンドユーザーに署名済み設定ファイルを送信することもできます。暗号化サービスアカウントで管理者としてリストされているメッセージ電子メールアドレスを送信する必要があります。

（注） メーリング リスト宛てに、署名された BCE Config ファイルを送らないでください。暗号化サービスはメーリングリストをサポートしていません。

Cisco Secure Email Encryption Plug-in の設定

Cisco Secure Email Encryption Plug-in をインストールすると、Outlook の [Cisco Secure Email Encryption] タブから設定を変更できるようになります。

- 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 Encryption] に移動します。

Encryption Plug-in のインストールは変更が可能です。または、両方のプラグインのインストールに影響する汎用オプションを変更できます。たとえば、Cisco Secure Email Encryption Plug-in のロギングを有効または無効にしたり、特定の暗号化モードのオプションを変更できます。

暗号化する電子メールのマーキング方法を変更するには、*BCE_Config.xml* ファイルを変更して、自動設定を実行する必要があります。設定を指定する場合、それらの設定にはCisco Secure Email Gateway との互換性が必要です。

Outlook の設定を変更する場合は、Cisco Secure Email Encryption Plug-in for Outlook の設定と使用を参照してください。

Cisco Secure Email Encryption Plug-in に必要なシステムプロセス

Cisco Secure Email Encryption Plug-in で必要なものは、TCP/IP DNS や DHCP などの必須のシステムプロセスのみで、これらのものは無効にすることはできません。ただし、データベースマネージャ、HTTP サーバー、ハードウェア設定デーモンなどの必須ではないシステムプロセスは、Cisco Email Encryption Plug-in の機能に影響を与えずに無効にすることができます。

Cisco Secure Email EncryptionPlug-in に必要な TCP サービス

ネットワークで次のTCPサービスとファイアウォールポートを開いていることを確認します。

デフォルト ポート	プロトコル	ホストネーム	目的
53	DNS	res.cisco.com	Encryption Service キーサーバーの URL を解決するには、DNSが必要です。 すべてのエンドユーザーがこのサービスにアクセスできる必要があります。
443	HTTPS	-	モードが暗号化、フラグ、および復号（デフォルト）の Encryption Service サーバーにアクセスするには、HTTPSが必要です。
		res.cisco.com	認証
		verify.res.cisco.com	BCE構成ファイルの署名（初回の場合）。
		updates.res.cisco.com	プラグインの更新の場合。

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。