Cisco 電子メール暗号化

この章は、次の項で構成されています。

Cisco 電子メール暗号化の概要

AsyncOS は暗号化を使用して着信電子メールと発信電子メールをサポートします。この機能を使用するには、暗号化されたメッセージの特性およびキー（鍵）サーバの接続性の情報を指定する暗号化プロファイルを作成します。キーサーバは、次のいずれかであると考えられます。

- Cisco Registered Envelope Service（マネージド サービス）、または
- Cisco 暗号化アプライアンス（ローカルの管理対象サーバ）

次に、暗号化するメッセージを作成するために、コンテンツ フィルタ、メッセージ フィルタ、データ漏洩防止ポリシーを作成します。

1. フィルタ条件に合致する発信メッセージは、電子メールゲートウェイの暗号化処理のキューに入れられます。
2. メッセージが暗号化されると、暗号化に使われたキーが暗号化プロファイルで指定されたキー サーバに保存され、暗号化されたメッセージが配信のキューに入れられます。
3. キューの中の電子メールの暗号化を妨げるような条件（つまり、一時的なCシリーズのビジー状態や Cisco Secure Email Encryption サービスが使用できない状態）が一時的に存在すると、メッセージはキューに入れられ、しばらくしてから再度暗号化が試行されます。

（注） また、メッセージを暗号化する前に、まずTLS接続経由で送信を試みるように電子メールゲートウェイを設定することもできます。詳細については、TLS接続を暗号化の代わりに使用 （10 ページ）を参照してください。

ローカル キー サーバで暗号化する方法

表 *1*: ローカル キー サーバで暗号化する方法

手順	操作内容	詳細
ステップ 1	ネットワークの Cisco IronPort 暗号化アプライアンスを設定します。	セットアップおよび設置を参照してください。
ステップ 2	メッセージ暗号化をイネーブルにします。	電子メールゲートウェイでのメッセージの暗号化のイネーブル化 （4 ページ）。
ステップ 3	暗号化プロファイルを作成して、暗号化されたメッセージにセキュリティ設定を使用するための暗号キー サーバを指定します。	キー サービスによる暗号化メッセージの処理方法の設定 （4 ページ）。
ステップ 4	電子メールゲートウェイが暗号化できるように、メッセージが満たす必要のある条件を定義します。	暗号化するメッセージの決定 （10 ページ）。
ステップ 5	電子メールのワークフローにおいてメッセージを暗号化するタイミングを決定します。	• コンテンツ フィルタを使用したメッセージの暗号化と即時配信 （11 ページ）。 または • コンテンツ フィルタを使用した配信時のメッセージの暗号化 （12 ページ）。
ステップ 6	（任意）メッセージに追加セキュリティのフラグを付けます。	メッセージへの暗号化ヘッダーの挿入 （13 ページ）。
ステップ 7	メッセージを暗号化するユーザ グループを定義します。	メール ポリシーを作成します。 メール ポリシーを参照してください
ステップ 8	定義したユーザ グループに定義済みの暗号化アクションを関連付けます。	メール ポリシーにコンテンツ フィルタを関連付けます。 メール ポリシーを参照してください

関連項目

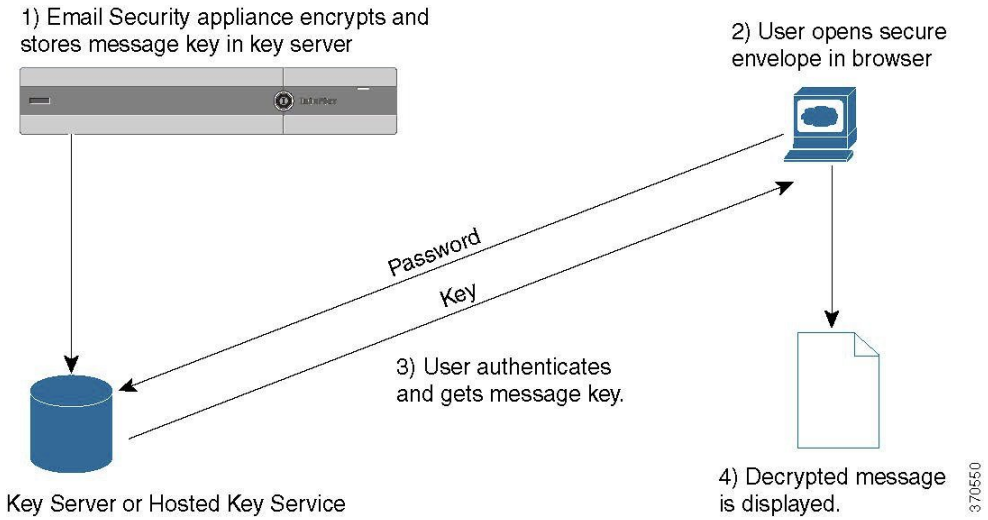
- 暗号化ワークフロー （2 ページ）

暗号化ワークフロー

電子メール暗号化を使用する場合、電子メールゲートウェイはメッセージを暗号化し、ローカルキーサーバまたはホステッドキーサービスにメッセージキーを格納します受信者が暗号化さ

れたメッセージを開封すると、キーサービスによって受信者が認証され、復号されたメッセージが表示されます。

図 *1*:暗号化ワークフロー



暗号化されたメッセージを開封する基本的なワークフローは次のとおりです。

1. 暗号化プロファイルを設定するときは、メッセージ暗号化のパラメータを指定します。暗号化されたメッセージでは、メッセージキーが電子メールゲートウェイによりローカルキーサーバ、またはホステッドキーサービス（Cisco Registered Envelope Service）に作成および格納されます。
2. 受信者はブラウザで安全なエンベロープを開封します。
3. ブラウザで暗号化されたメッセージを開封するとき、受信者の本人確認のためパスワードが必要となります。キー サーバはメッセージに関連付けられた暗号化キーを返します。

> **注** 暗号化された電子メール メッセージの初回開封時に、受信者は安全なエンベロープを開封するためのキー サービスに登録する必要があります。登録後、暗号化プロファイルの設定によっては、受信者が暗号化されたメッセージを認証なしで開封することも可能です。暗号化プロファイルでは、パスワード不要と指定できますが、特定の機能が使用できなくなります。

4. 復号したメッセージが表示されます。

電子メールゲートウェイを使用したメッセージの暗号化

電子メールゲートウェイによる暗号化を使用するには、暗号化プロファイルを設定する必要があります。encryptionconfig CLI コマンド、または GUI の [セキュリティサービス（Security Services）] > [Cisco IronPortメール暗号化（Cisco IronPort Email Encryption）] で、暗号化プロファイルをイネーブルにして設定することができます。

（注） 電子メールゲートウェイで PXE 暗号化と S/MIME 暗号化が有効になっている場合、AsyncOS ではまず S/MIME を使用して、次に PXE を使用してメッセージが暗号化されます。

関連項目

- 電子メールゲートウェイでのメッセージの暗号化のイネーブル化 （4 ページ）
- キー サービスによる暗号化メッセージの処理方法の設定 （4 ページ）
- エンベロープのデフォルト ロケールの設定 （8 ページ）
- PXE エンジンの最新バージョンへの更新 （9 ページ）

電子メールゲートウェイでのメッセージの暗号化のイネーブル化

手順

ステップ 1 [セキュリティサービス（Security Services）] > [Cisco IronPort電子メール暗号化（Cisco IronPort Email Encryption）] をクリックします。

ステップ 2 [有効（Enable）] をクリックします。

ステップ 3 （任意）次のオプションを設定するには、[設定の編集（Edit Settings）] をクリックしてください。

- 暗号化する最大メッセージ サイズ。シスコが推奨するメッセージ サイズは 10 MB です。電子メールゲートウェイが暗号化するメッセージの最大サイズは 25 MB です。

  （注） 推奨される 10 MB の制限を超えてメッセージを暗号化すると、電子メールゲートウェイのパフォーマンスが遅くなる可能性があります。Cisco Registered Envelope サービスを使用する場合、メッセージ受信者は 10 MB より大きい添付ファイルのある暗号化メッセージへは返信できません。

- 暗号化アカウント管理者のメールアドレス。暗号化プロファイルをプロビジョニングすると、この電子メール アドレスが自動的に暗号化サーバに登録されます。

- プロキシ サーバを設定します。

キー サービスによる暗号化メッセージの処理方法の設定

キー サービスを使用する場合、1 つ以上の暗号化プロファイルを作成できます。さまざまな電子メール グループに異なるセキュリティ レベルを使用する場合、それぞれ別の暗号化プロファイルを作成することもできます。たとえば、機密資料を含んだメッセージを高レベルのセキュリティで送信し、他のメッセージを中レベルのセキュリティで送信するという場合です。この場合、特定のキー ワード（「confidential」など）を含むメッセージには高レベルのセキュリ

ティ暗号化プロファイルを作成し、他の発信メッセージには別の暗号化プロファイルを作成します。

暗号化プロファイルをカスタム ユーザ ロールに割り当て、そのロールに割り当てられた委任管理者が DLP ポリシーとコンテンツ フィルタで暗号化プロファイルを使用できるようにします。DLP ポリシーとコンテンツ フィルタを設定する場合は、管理者、オペレータ、および委任ユーザだけが暗号化プロファイルを使用できます。カスタム ロールに割り当てられない暗号化プロファイルは、メールまたは DLP ポリシー権限を持つすべての委任管理者が使用できます。詳細については、管理タスクの分散を参照してください。

（注） 1 つのホステッド キー サービスに複数の暗号化プロファイルを設定できます。組織に複数のブランドがある場合、PXE エンベロープ用にキー サーバに格納された異なるロゴを参照することができます。

暗号化プロファイルは次の設定を保存します。

- [キーサーバ設定（Key server settings）]。キー サーバとそのキー サーバに接続するための情報を指定します。
- [エンベロープ設定（Envelope settings）]。セキュリティ レベル、開封確認を返すか、暗号化キューにあるメッセージがタイムアウトするまでの時間、使用する暗号化アルゴリズムのタイプ、および復号アプレットをブラウザで動作可能にするかなど、メッセージエンベロープの詳細を指定します。
- [メッセージ設定（Message settings）]。安全なメッセージ転送や安全な「全員に返信」をイネーブルにするかなど、メッセージに関する詳細を指定します。
- [通知設定（Notification settings）]。暗号化失敗通知と同様、テキスト形式および HTML 形式の通知を使う通知テンプレートを指定します。暗号化プロファイル作成時に、テキスト リソース内のテンプレートを作成し、テンプレートを選択します。エンベロープをローカライズし、暗号化失敗通知のメッセージの件名を指定することもできます。通知の詳細については、暗号化通知テンプレートおよびバウンス通知および暗号化失敗通知テンプレートを参照してください。

手順

ステップ 1 [メール暗号化プロファイル（Email Encryption Profiles）] のセクションで [暗号化プロファイルの追加（Add Encryption Profile）] をクリックします。

ステップ 2 暗号化プロファイルの名前を入力します。

ステップ 3 [使用者（役割）（Used By (Roles)）] リンクをクリックし、暗号化プロファイルへのアクセス権を設定するカスタム ユーザ ロールを選択して、[OK] をクリックします。

このカスタム ロールに割り当てられた委任管理者は、責任があるすべての DLP ポリシーとコンテンツ フィルタに対して暗号化プロファイルを使用できます。

ステップ 4 [キー サーバ設定（Key Server Settings）] セクションで次のキー サーバから選択します。

- Cisco 暗号化アプライアンス（ネットワーク内）

- Cisco Registered Envelope Service（ホスト キー サービス）

ステップ 5 Cisco暗号化アプライアンス（ローカル キー サービス）を選択した場合は、次の設定を入力します。

- **[内部URL（Internal URL）]。**電子メールゲートウェイは、この URL を使用してネットワーク内の Cisco 暗号化アプライアンスと通信します。
- [外部URL（External URL）]。受信者のメッセージは、この URL を使用して Cisco 暗号化アプライアンスのキーおよび他のサービスにアクセスします。受信者は、受信HTTPまたは HTTPS 要求をするためにこの URL を使用します。

ステップ 6 Cisco Registered Envelope Service を選択した場合は、ホステッド キー サービスの URL を入力します。キー サービスの URL は、https://res.cisco.com です。

ステップ 7 [キーサーバ設定（Key Server Settings）] で [詳細（Advanced）] をクリックし、受信者がエンベロープを開封した場合、エンベロープの暗号化ペイロードの転送に HTTP または HTTPS を使用するかどうかを指定します。次のいずれかを選択してください。

- [キーサービスをHTTPで使用する（Use the Key Service with HTTP）]。受信者がエンベロープを開封すると、HTTP を使用してキー サービスから暗号化ペイロードを転送します。Cisco Registered Envelope Service を使用する場合は、これはステップ 6 で指定した URL です。Cisco暗号化アプライアンスを使用する場合は、これはステップ5で指定した外部URLです。
- ペイロードがすでに暗号化されているため、HTTPに転送しても安全であり、HTTPSに送信するよりも迅速です。これは、HTTPS経由でイメージ要求を送信するよりも、パフォーマンスがさらに向上します。
- [キーサービスをHTTPSで使用する（Use the Key Service with HTTPS）]。受信者がエンベロープを開封すると、HTTPS を使用してキー サービスから暗号化ペイロードを転送します。Cisco Registered Envelope Service を使用する場合は、これはステップ 6 で指定したURLです。Cisco 暗号化アプライアンスを使用する場合は、これはステップ 5 で指定した外部 URL です。
- [ペイロードトランスポートの個別のURLを指定します（Specify a separate URL for payload transport）]。暗号化ペイロードにキー サーバを使用しない場合は、ペイロード転送には HTTP または HTTPS を使用するかどうかを別の URL を使用して指定できます。

ステップ 8 [エンベロープ設定（Envelope Settings）] のセクションで、メッセージのセキュリティ レベルを選択します。

- [セキュリティ（高）（High Security）]。受信者は、暗号化されたメッセージを開封するには、パスフレーズを必ず入力する必要があります。
- [セキュリティ（中）（Medium Security）]。受信者の資格情報がキャッシュされていれば、受信者は暗号化されたメッセージを開封するために資格情報を入力する必要はありません。

- [パスフレーズは不要です（No Passphrase Required）]。暗号化されたメッセージの最も低いセキュリティ レベルです。暗号化されたメッセージを開封するために受信者がパスフレーズを入力する必要はありません。それでも、パスフレーズ保護されないエンベロープの [開封確認（Read Receipts）]、[全員への安全な返信（Secure Reply All）]、および [メッセージの安全な転送（Secure Message Forwarding）] 機能を有効にできます。

ステップ 9 ユーザが組織のロゴをクリックするとその組織の URL が開くようにするように、ロゴのリンクを追加できます。次のオプションから選択します。

- **[リンクなし（No link）]。**実際のリンクは、メッセージエンベロープに追加されません。
- [カスタムリンクURL（Custom link URL）]。URL を入力し、メッセージ エンベロープへの実際のリンクを追加します。

ステップ 10 （任意）開封確認をイネーブルにします。このオプションをイネーブルにすると、受信者が安全なエンベロープを開くと、送信者は開封確認を受信します。

ステップ 11 （任意）次の設定を行うために、任意で [エンベロープ設定（Envelope Settings）] の [詳細設定（Advanced）] をクリックしてください。

- 暗号化キューにあるメッセージがタイムアウトするまでの時間（秒単位）を入力します。メッセージがタイムアウトになると、電子メールゲートウェイはメッセージをバウンスし、送信者に通知を送信します。
- 暗号化アルゴリズム「AES 192」または「AES 256」 を選択します。

  （注） AESは、より強力な暗号化を実現しますが、復号により長い時間がかかるため、受信者には遅延が発生します。AESは、通常、政府や銀行業務のアプリケーションで使用されます。

- 復号アプレットをイネーブルまたはディセーブルにします。このオプションをイネーブルにすると、メッセージの添付ファイルがブラウザ環境で開かれるようになります。このオプションをディセーブルにすると、メッセージの添付ファイルがキーサーバで復号されるようになります。ディセーブルの場合、メッセージの開封により時間がかかるようになりますが、ブラウザ環境に依存しなくなります。

ステップ 12 [メッセージ設定（Message settings）] セクションで、次のようにします。

- 全員へのセキュアな返信機能をイネーブルにするには、[全員にセキュアな返信を有効にする（Enable Secure Reply All）] チェックボックスをオンにします。
- セキュアなメッセージ転送機能をイネーブルにするには、[セキュアなメッセージ転送を有効にする（Enable Secure Message Forwarding）] チェックボックスをオンにします。

ステップ 13 （任意）Cisco Registered Envelope Service を選択しており、このサービスでエンベロープのローカリゼーションがサポートされている場合は、エンベロープのローカリゼーションをイネーブルにします。[通知設定（Notification Settings）] セクションで [ローカライズされたエンベロープの使用（Use Localized Envelope）] チェックボックスをオンにします。

（注） エンベロープのローカリゼーションをイネーブルにすると、暗号化されたメッセージの HTML またはテキストによる通知を選択できません。

エンベロープのデフォルト ロケールを設定する場合は、エンベロープのデフォルト ロケールの設定 （8 ページ）を参照してください。

ステップ 14 HTML 形式またはテキスト形式の通知テンプレートを選択します。

（注） キー サーバは、受信者の電子メール アプリケーションによって、HTML またはテキスト形式の通知を使います。両方の通知を設定する必要があります。

次の手順を実行します。

a) HTML 形式の通知テンプレートを選択します。テキスト リソースで設定した HTML 形式の通知から選択します。テンプレートが設定されていなかった場合、システムはデフォルトのテンプレートを使用します。

b) テキスト形式の通知テンプレートを選択します。テキスト リソースで設定したテキスト形式の通知から選択します。テンプレートが設定されていなかった場合、システムはデフォルトのテンプレートを使用します。

（注） これらのオプションは、ローカライズされたエンベロープを使用している場合には使用できません。

ステップ 15 暗号化失敗通知用の件名ヘッダーを入力します。暗号化プロセスがタイムアウトした場合、電子メールゲートウェイは通知を送信します。

ステップ 16 メッセージ本文の暗号化失敗通知テンプレートを選択します。テキスト リソースで設定した暗号化失敗通知テンプレートから選択します。テンプレートが設定されていなかった場合、システムはデフォルトのテンプレートを使用します。

ステップ 17 変更を送信し、保存します。

ステップ 18 Cisco Registered Envelope Service を使用する場合、電子メールゲートウェイをプロビジョニングする手順を追加で実行する必要があります。電子メールゲートウェイをプロビジョニングすると、暗号化プロファイルがホステッドキーサービスと共に登録されます。電子メールゲートウェイをプロビジョニングするには、登録する暗号化プロファイルの [プロビジョニング（Provision）] ボタンをクリックします。

エンベロープのデフォルト ロケールの設定

エンベロープのデフォルト ロケールは英語です。Cisco Registered Envelope Service を選択しており、このサービスでエンベロープのローカリゼーションがサポートされている場合は、エンベロープのロケールを次のいずれかに変更できます。

- 英語
- フランス語
- ドイツ語
- 日本語

- ポルトガル語
- スペイン語
- イタリア語
- 韓国語
- オランダ語
- ポーランド語
- ロシア語
- 中国語

はじめる前に

- キー サービス タイプとして Cisco Registered Envelope Service を使用し、エンベロープのローカリゼーションがイネーブルな状態で、暗号化プロファイルを作成します。キー サービスによる暗号化メッセージの処理方法の設定 （4 ページ）を参照してください。
- Cisco Registered Envelope Service でエンベロープのローカリゼーションがサポートされていることを確認します。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [Cisco IronPort電子メール暗号化（Cisco IronPort Email Encryption）] をクリックします。

ステップ 2 既存の暗号化プロファイルを開きます。

ステップ 3 [通知設定（Notification Settings）] セクションの [ローカライズされたエンベロープ（Localized Envelopes）] ドロップダウンリストからロケールを選択します。

ステップ 4 **[送信（Submit）]** をクリックします。

ステップ 5 [変更を確定（Commit Changes）] をクリックします。

PXE エンジンの最新バージョンへの更新

[Ciscoメール暗号化設定（Cisco Email Encryption Settings）] ページには、PXE エンジンの現在のバージョンおよび電子メールゲートウェイで使用するドメインマッピングファイルが表示されます。[セキュリティサービス（Security Services）] > [サービスアップデート（Service Updates）] ページ（または CLI の updateconfig コマンド）を使って、自動的に PXE エンジンを更新するように電子メールゲートウェイを設定できます。詳細については、サービス アップデートを参照してください。

また、[IronPortメール暗号化設定（IronPort Email Encryption Settings）] ページの [PXEエンジンの更新（PXE Engine Updates）] セクションの [今すぐ更新（Update Now）] ボタン（または CLI の **encryptionupdate** コマンド）を使用して、手動でエンジンを更新することもできます。

暗号化するメッセージの決定

暗号化プロファイルの作成後、どの電子メールメッセージを暗号化すべきかを決める発信コンテンツフィルタを作成する必要があります。コンテンツフィルタは、発信電子メールをスキャンしてメッセージが指定された条件に一致するか判断します。コンテンツフィルタによりメッセージが条件に一致すると判断されたら、電子メールゲートウェイはメッセージを暗号化し、生成されたキーをキーサーバに送信します。このアプライアンスは、使用するキーサーバを決定するための、暗号化プロファイルで指定された設定と、他の暗号化設定を使用します。

データ漏洩防止スキャン後に解放された後でも、メッセージを暗号化できます。詳細については、DLP 違反アクション（メッセージ アクション）に対して実行するアクションの定義を参照してください。

関連項目

- TLS 接続を暗号化の代わりに使用 （10 ページ）
- コンテンツ フィルタを使用したメッセージの暗号化と即時配信 （11 ページ）
- コンテンツ フィルタを使用した配信時のメッセージの暗号化 （12 ページ）

TLS 接続を暗号化の代わりに使用

ドメイン用に指定された送信先コントロールに基づき、電子メールゲートウェイは、メッセージを暗号化する代わりに TLS 接続を介してメッセージをセキュアにリレーできます（TLS 接続が使用可能な場合）。電子メールゲートウェイは、送信先コントロール（必須（Required）、推奨（Preferred）、またはなし（None））の TLS 設定と暗号化コンテンツフィルタで定義されたアクションに基づいて、メッセージを暗号化するか TLS 接続で送信するか決定します。

コンテンツ フィルタ作成時に、必ずメッセージを暗号化するか、まず TLS 接続で送信を試みて、TLS 接続が使用不可であればメッセージを暗号化するかを指定できます。次の表では、暗号化制御フィルタが最初に TLS 接続でのメッセージの送信を試みる場合、 電子メールゲートウェイが、ドメインの送信先コントロールの TLS 設定に基づいてどのようにメッセージを送信するかを示しています。

表 *2:* 電子メールゲートウェイの *TLS* サポート

送信先コントロール TLS 設定	TLS 接続が使用可能である場合のアクション	TLS 接続が使用不可である場合のアクション
なし	エンベロープを暗号化して送信します。	エンベロープを暗号化して送信します。
TLS 推奨	TLS 経由で送信します。	エンベロープを暗号化して送信します。
TLS 必須	TLS 経由で送信します。	リトライまたはメッセージのバウンス

送信先コントロールで TLS をイネーブルにする方法については、電子メールを受信するためのゲートウェイの設定を参照してください。

コンテンツ フィルタを使用したメッセージの暗号化と即時配信

はじめる前に

- コンテンツ フィルタを構築するための条件の概念を理解するには、コンテンツ フィルタの概要を参照してください。
- （任意）メッセージへの暗号化ヘッダーの挿入 （13 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [発信コンテンツフィルタ（Outgoing Content Filters）] に移動します。

ステップ 2 [フィルタ（Filters）] セクションで、[フィルタを追加（Add Filter）] をクリックします。

ステップ 3 [条件（Conditions）] セクションで、[条件を追加（Add Condition）] をクリックします。

ステップ 4 暗号化するメッセージをフィルタリングする条件を追加します。たとえば、機密資料を暗号化するために、件名または本文に特定の単語またはフレーズ（「Confidential」など）を含むメッセージを識別する条件を追加できます。

ステップ 5 [OK] をクリックします。

ステップ 6 任意で、[アクションを追加（Add Action）] をクリックし、[ヘッダーの追加（Add Header）] を選択し、追加の暗号化設定を指定する暗号化ヘッダーをメッセージに挿入します。

ステップ 7 [アクション（Actions）] セクションで、[アクションを追加（Add Action）] をクリックします。

ステップ 8 [アクションを追加（Add Action）] リストから [暗号化して今すぐ配信(最終アクション)（Encrypt and Deliver Now (Final Action)）] を選択します。

ステップ 9 条件に合致するメッセージを常に暗号化するか、TLS 接続を介した送信の試行が失敗したときのみメッセージを暗号化するかを選択します。

ステップ 10 コンテンツ フィルタに関連付ける暗号化プロファイルを選択します。

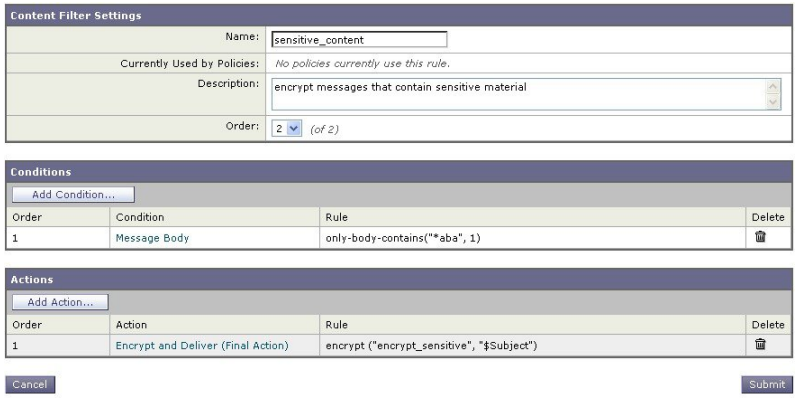
暗号化プロファイルは、使用するキー サーバ、セキュリティ レベル、およびメッセージ エンベロープのフォーマット化に関する設定、および他のメッセージ設定を指定します。暗号化プロファイルをコンテンツ フィルタに関連付けた場合、コンテンツ フィルタはこれらの格納された設定を暗号化メッセージに使用します。

ステップ 11 メッセージの件名を入力します。

ステップ 12 [OK] をクリックします。

次の図のコンテンツ フィルタは、メッセージ本文で ABA コンテンツを検索するコンテンツ フィルタを示します。コンテンツ フィルタで定義されているアクションは、電子メールを暗号化して配信すると指定しています。

図 *2:* 暗号化コンテンツ フィルタ



ステップ 13 暗号化アクションを追加した後、[送信（Submit）] をクリックします。

ステップ 14 変更を保存します。

次のタスク

コンテンツ フィルタを追加したら、フィルタを発信メール ポリシーに追加する必要があります。組織のニーズに応じて、デフォルト ポリシーでコンテンツ フィルタをイネーブルにする、またはフィルタを特定のメール ポリシーに適用することを選択します。メール ポリシーの操作については、メール ポリシーの概要を参照してください。

コンテンツ フィルタを使用した配信時のメッセージの暗号化

配信時にメッセージを暗号化するコンテンツ フィルタを作成するには、次の手順に従ってください。配信時の暗号化とは、メッセージが次の処理の段階に進み、すべての処理が完了した時点で、メッセージが暗号化され、配信されることを意味します。

はじめる前に

- コンテンツ フィルタを構築するための条件の概念を理解するには、コンテンツ フィルタの概要を参照してください。
- （任意）メッセージへの暗号化ヘッダーの挿入 （13 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [発信コンテンツフィルタ（Outgoing Content Filters）] に移動します。

ステップ 2 [フィルタ（Filters）] セクションで、[フィルタを追加（Add Filter）] をクリックします。

ステップ 3 [条件（Conditions）] セクションで、[条件を追加（Add Condition）] をクリックします。

ステップ 4 暗号化するメッセージをフィルタリングする条件を追加します。たとえば、機密資料を暗号化するために、件名または本文に特定の単語またはフレーズ（「Confidential」など）を含むメッセージを識別する条件を追加できます。

ステップ 5 [OK] をクリックします。

ステップ 6 任意で、[アクションを追加（Add Action）] をクリックし、[ヘッダーの追加（Add Header）] を選択し、追加の暗号化設定を指定する暗号化ヘッダーをメッセージに挿入します。

ステップ 7 [アクション（Actions）] セクションで、[アクションを追加（Add Action）] をクリックします。

ステップ 8 [アクションを追加（Add Action）] リストから [配信時の暗号化（Encrypt on Delivery）] を選択します。

ステップ 9 条件に合致するメッセージを常に暗号化するか、TLS 接続を介した送信の試行が失敗したときのみメッセージを暗号化するかを選択します。

ステップ 10 コンテンツ フィルタに関連付ける暗号化プロファイルを選択します。

暗号化プロファイルは、使用するキー サーバ、セキュリティ レベル、およびメッセージ エンベロープのフォーマット化に関する設定、および他のメッセージ設定を指定します。暗号化プロファイルをコンテンツ フィルタに関連付けた場合、コンテンツ フィルタはこれらの格納された設定を暗号化メッセージに使用します。

ステップ 11 メッセージの件名を入力します。

ステップ 12 [OK] をクリックします。

ステップ 13 暗号化アクションを追加した後、[送信（Submit）] をクリックします。

ステップ 14 変更を保存します。

次のタスク

コンテンツ フィルタを追加したら、フィルタを発信メール ポリシーに追加する必要があります。組織のニーズに応じて、デフォルト ポリシーでコンテンツ フィルタをイネーブルにする、またはフィルタを特定のメール ポリシーに適用することを選択します。メール ポリシーの操作については、メール ポリシーの概要を参照してください。

メッセージへの暗号化ヘッダーの挿入

AsyncOS では、コンテンツ フィルタまたはメッセージ フィルタを使って SMTP ヘッダーをメッセージに挿入することで、暗号化設定をメッセージに追加できます。暗号化ヘッダーは、関連付けられた暗号化プロファイルで定義されている暗号化設定を上書きすることが可能で、指定された暗号化機能をメッセージに適用できます。

（注） Cisco 暗号化アプライアンスはフラグ付きのメッセージを処理するように設定する必要があります。

手順

ステップ 1 [メールポリシー（Mail Policies）]>[発信コンテンツフィルタ（Outgoing Content Filters）]または[受信コンテンツフィルタ（Incoming Content Filters）]に進みます。

ステップ 2 [フィルタ（Filters）]セクションで、[フィルタを追加（Add Filter）]をクリックします。

ステップ 3 [アクション（Actions）]セクションで、[アクションを追加（Add Action）]をクリックして[ヘッダーの追加/編集（ヘッダーの追加/編集）]を選択し、追加の暗号化設定を指定するためにメッセージに暗号化ヘッダーを挿入します。

たとえば、Registered Envelope を送信後 24 時間で期限切れにする場合は、ヘッダー名として X-PostX-ExpirationDate、ヘッダーの値として +24:00:00 を入力します。

次のタスク

関連項目

- 暗号化ヘッダー （14 ページ）
- 暗号化ヘッダーの例 （16 ページ）
- 暗号化コンテンツ フィルタの作成の詳細については、コンテンツ フィルタを使用したメッセージの暗号化と即時配信 （11 ページ）を参照してください。
- メッセージ フィルタを使用したヘッダー挿入については、メッセージ フィルタを使用した電子メール ポリシーの適用を参照してください。

暗号化ヘッダー

次の表に、メッセージに追加可能な暗号化ヘッダーを示します。

表 *3*: 電子メール暗号化ヘッダー

MIME ヘッダー	説明	値
`X-PostX-Reply- Enabled`	メッセージで安全な返信をイネーブルにするかを示し、メッセージ バーに[返信（Reply）]ボタンを表示します。このヘッダーは、メッセージに暗号化設定を追加します。	[返信（Reply）]ボタンを表示または非表示にするかを示すブール値。true に設定するとボタンを表示します。デ フォルト値は true です。
`X-PostX-Reply-All-Enabled`	メッセージで安全な「全員に返信」をイネーブルにするかを示し、メッセージ バーに[全員に返信（Reply All）]ボタンを表示します。このヘッダーは、デフォルトのプロファイル設定を上書きします。	[全員に返信（Reply All）]ボタンを表示または非表示にするかを示すブール値。true に設定するとボタンを表示します。デ フォルト値は true です。

MIME ヘッダー	説明	値
X-PostX-Forward-Enabled	メッセージの安全な転送をイネーブルにするかを示し、メッセージ バーに [転送（Forward）] ボタンを表示します。このヘッダーは、デフォルトのプロファイル設定を上書きします。	[転送（Forward）] ボタンを表示または非表示にするかを示すブール値。true に設定するとボタンを表示します。デフォルト値は true です。
X-PostX-Send-Return-Receipt	開封確認をイネーブルにするかを示します。受信者が安全なエンベロープを開くと、送信者は開封確認を受信します。このヘッダーは、デフォルトのプロファイル設定を上書きします。	開封確認を送信するかしないかを示すブール値。true に設定するとボタンを表示します。デ フォルト値は true です。
X-PostX-Expiration Date	送信前に Registered Envelope の有効期限の日付を設定します。有効期限後は、キー サーバにより Registered Envelope へのアクセスが制限されます。Registered Envelope は、メッセージの期限が切れたというメッセージを表示します。このヘッダーは、メッセージに暗号化設定を追加します。 Cisco Registered Envelope Service を使用している場合、メッセージ送信後に http://res.cisco.com の Web サイトにログインして、メッセージ管理機能でメッセージの有効期限を設定、調整、削除できます。	相対的な日付や時間を含む文字列値。相対的な時間、分、秒には +HH:MM:SS 形式、相対的な日付には +D 形式を使います。デフォルトでは、有効期限はありません。
X-PostX-ReadNotification Date	送信前に Registered Envelope の「開封期限」の日付を設定します。Registered Envelope がこの期限までに読まれなかった場合、ローカル キー サーバは通知を生成します。このヘッダーを持つ Registered Envelope は、Cisco Registered Envelope Service では機能せず、ローカル キー サーバでのみ機能します。このヘッダーは、メッセージに暗号化設定を追加します。	相対的な日付や時間を含む文字列値。相対的な時間、分、秒には +HH:MM:SS 形式、相対的な日付には +D 形式を使います。デフォルトでは、有効期限はありません。
X-PostX-Suppress-Applet-For-Open	復号アプレットをディセーブルにするかしないかを示します。復号アプレットにより、ブラウザ環境でメッセージの添付ファイルが開かれます。アプレットをディセーブルにすると、メッセージの添付ファイルはキー サーバで復号されます。このオプションをディセーブルにすると、メッセージの開封により時間がかかるようになりますが、ブラウザ環境に依存しなくなります。このヘッダーは、デフォルトのプロファイル設定を上書きします。	復号アプレットをディセーブルにするかしないかのブール値。アプレットをディセーブルにするには true に設定します。デ フォルト値は true です。

MIME ヘッダー	説明	値
X-PostX-Use-Script	JavaScript を含まないエンベロープを送信するかしないかを示します。JavaScript を含まないエンベロープとは、受信者のコンピュータ上でエンベロープをローカルに開封するために使われる JavaScript を含まない Registered Envelope のことです。受信者は、メッセージを見るには Open Online メソッド、または Open by Forwarding メソッドのいずれかを使用する必要があります。受信者のドメインのゲートウェイにより JavaScript が削除され、暗号化されたメッセージを開封できない場合、このヘッダーを使います。このヘッダーはメッセージに暗号化設定を追加します。	JavaScript アプレットを含めるか含めないかのブール値。JavaScript を含まないエンベロープを送信するには、false に設定します。デフォルト値は true です。
X-PostX-Remember-Envelope-Key-Checkbox	オフラインでエンベロープを開封するため、エンベロープ固有のキーのキャッシュを許可するかしないかを示します。エンベロープ キーのキャッシングでは、受信者が正しいパスフレーズを入力し、[このエンベロープのパスワードを記憶する（Remember the password for this envelope）] チェックボックスをオンにした場合、個別のエンベロープの復号キーが受信者のコンピュータでキャッシュされます。これ以降、受信者はそのコンピュータでエンベロープを再開封するためにパスフレーズをもう一度入力する必要はありません。このヘッダーは、メッセージに暗号化設定を追加します。	エンベロープ キーのキャッシュをイネーブルにするか、[このエンベロープのパスワードを記憶する（Remember the password for this envelope）] チェックボックスを表示するかしないかのブール値。デ フォルト値は true です。

暗号化ヘッダーの例

この項では、暗号化ヘッダーの例を示します。

関連項目

- JavaScript を含まないエンベロープのイネーブル化 （17 ページ）
- オフラインでの開封のためエンベロープ キーをイネーブルにする （16 ページ）
- メッセージ有効期限のイネーブル化 （17 ページ）
- 復号アプレットの無効化 （17 ページ）

オフラインでの開封のためエンベロープ キーをイネーブルにする

エンベロープ キーのキャッシュをイネーブルにして Registered Envelope を送信するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-Remember-Envelope-Key-Checkbox: true
```

[このエンベロープのパスワードを記憶する（Remember the password for this envelope）] チェックボックスが Registered Envelope に表示されます。

JavaScript を含まないエンベロープのイネーブル化

JavaScript を含めずに Registered Envelope を送信するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-Use-Script: false
```

受信者が securedoc.html 添付ファイルを開くと、Registered Envelope が [オンラインで開く（Open Online）] リンクと共に表示され、[開く（Open）] ボタンがディセーブルになります。

メッセージ有効期限のイネーブル化

送信後、24 時間で有効期限が切れるようにメッセージを設定するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-ExpirationDate: +24:00:00
```

送信後 24 時間は、受信者はその暗号化されたメッセージを開封して内容を見ることができます。それ以降、Registered Envelope では、エンベロープの有効期限が切れたことを示すメッセージが表示されます。

復号アプレットの無効化

復号アプレットをディセーブルにし、メッセージの添付ファイルをキー サーバで復号するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-Suppress-Applet-For-Open: true
```

（注） 復号アプレットをディセーブルにしている場合、メッセージの開封には時間がかかりますが、ブラウザ環境には依存しなくなります。