CHAPTER 12

IronPort 電子メール暗号化

IronPort AsyncOS は、インバウンドおよびアウトバウンド電子メールをセキュリティ保護する暗号化に対応しています。

この章は、次の内容で構成されています。

IronPort 電子メール暗号化：概要

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、Cisco Registered Envelope Service（マネージド サービス）または IronPort 暗号化アプライアンス（ローカルのマネージド サーバ）のどちらでも可能です。次に、メッセージを暗号化するか決めるコンテンツ フィルタまたはメッセージ フィルタ（または両方）を作成します。

フィルタ条件に合致する発信メッセージは、電子メール セキュリティ アプライアンスの暗号化処理のキューに入れられます。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。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-Series のビジー状態や CRES 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アプライアンス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」（P.12-407）を参照してください。

電子メール セキュリティ アプライアンスでアウトバウンド電子メールの暗号化を設定するには、次の手順を実行します。

ステップ 1　**ローカル キー サーバを使用する場合は、IronPort 暗号化アプライアンスを構成します。**キー サーバを構成する手順については、『*IronPort Encryption Appliance Local Key Server User Guide*』を参照してください。

ステップ 2　**暗号化プロファイルを設定します。**暗号化プロファイルを設定する手順については、「電子メール暗号化プロファイルの設定」（P.12-400）を参照してください。

ステップ 3　**ホステッド キー サービスを使用するには、Cisco Registered Envelope Service コーポレート アカウントを作成します。暗号化プロファイルを設定した後、[Provision] ボタンをクリックしてアカウントを作成します。**

ステップ 4　**発信コンテンツ フィルタを設定します。**暗号化しなければならないアウトバウンド電子メールにタグをつけるように、コンテンツ フィルタを設定する必要があります。コンテンツ フィルタの作成手順については、「暗号化コンテンツ フィルタの設定」（P.12-406）を参照してください。

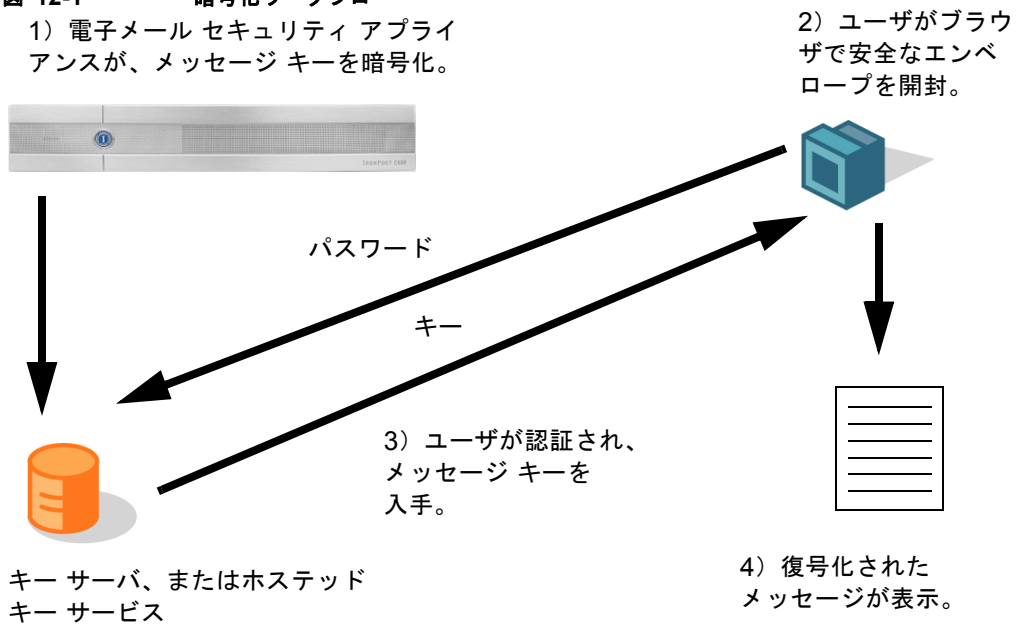
次の Web ブラウザがサポートされます。

- Microsoft® Internet Explorer 6（Windows のみ）
- Microsoft® Internet Explorer 7（Windows のみ）
- Firefox 2
- Firefox 3
- Safari 3

暗号化ワークフロー

電子メール暗号化を使用する場合、IronPort 電子メール セキュリティ アプライアンス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、復号化されたメッセージが表示されます。

図 12-1　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。

ステップ 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 セキュリティ アプライアンスによりローカル 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。

ステップ 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。

ステップ 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。

ステップ 4　復号化したメッセージが表示されます。

暗号化最大メッセージ サイズ

表 12-1 は、アプライアンスごとの暗号化可能な最大メッセージ サイズを示します。IronPort アプライアンスは、最大サイズを超過しているメッセージをバウンスします。

表 12-1　IronPort アプライアンスによる暗号化最大メッセージ サイズ

モデル	最大 メッセージ サイズ（MB）
C150/160	44
C350/360/370	46
C650/660/670 および X1050/1060/1070	50

電子メール暗号化プロファイルの設定

電子メール セキュリティ アプライアンス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 [Security Services] > [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。

電子メール暗号化グローバル設定の編集

電子メール暗号化をイネーブルにするには、次の手順を実行します。

ステップ 1　[Security Services] > [IronPort Email Encryption] をクリックします。

ステップ 2　[Enable] をクリックします。

ステップ 3　任意で、[Edit Settings] をクリックし、プロキシ サーバを設定します。

図 12-2　グローバル設定の構成

暗号化プロファイルの追加

ローカル キー サービスを使う場合、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。

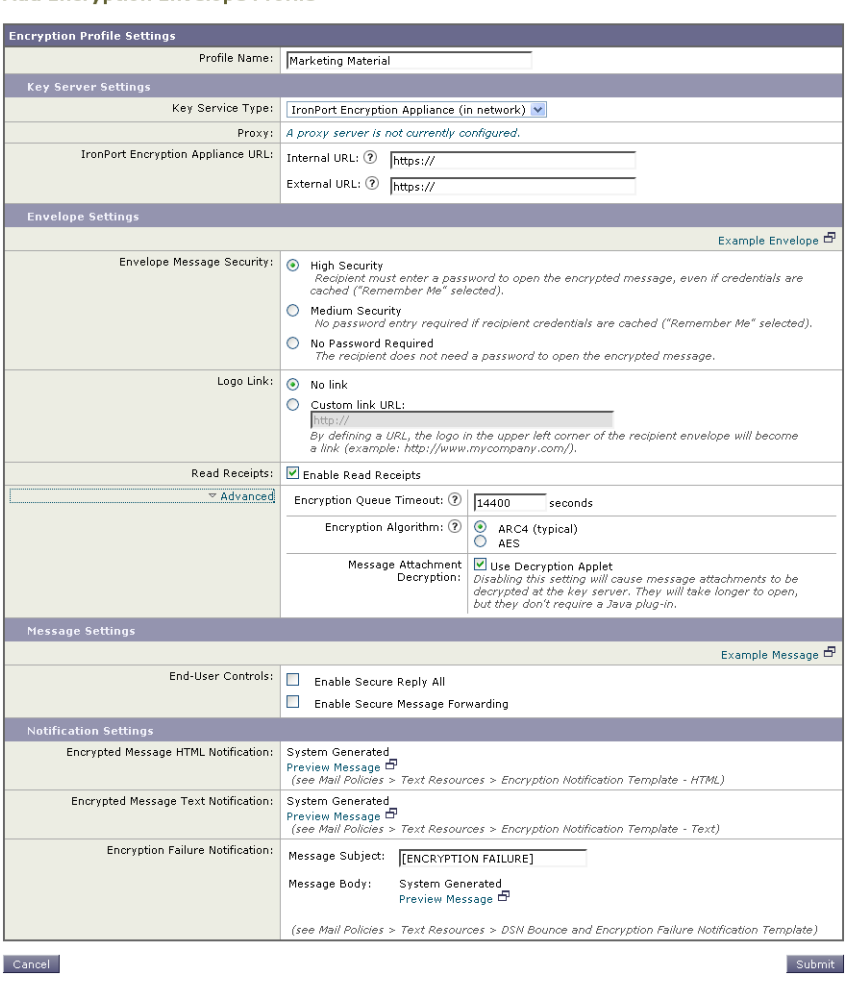
（注）　1 つのホステッド キー サービスに複数の暗号化プロファイルを設定できます。組織に複数のブランドがある場合、PXE エンベロープ用にキー サーバに格納された異なるロゴを参照することができます。

暗号化プロファイルを作成および保存し、次の暗号化の設定を保存します。

- [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。
- [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、および復号化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。

- [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。
- [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。暗号化失敗通知のメッセージの件名も指定できます。通知の詳細については、「暗号化通知テンプレート」（P.14-470）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」（P.14-464）を参照してください。

図 12-3　暗号化エンベロープ プロファイルの追加



暗号化プロファイルを追加するには次の手順に従ってください。

ステップ 1　[Email Encryption Profiles] のセクションで [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　[Key Server Settings] セクションで次のキー サーバから選択します。

- [IronPort Encryption appliance (in network)]
- [Cisco Registered Envelope Service (hosted key service)]

ステップ 4　[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 5　[IronPort Encryption appliance (local key service)] を選択した場合は、次の設定を入力します。

- [Internal URL]。IronPort 電子メール セキュリティ アプライアンスは、この URL でネットワーク内の IronPort 暗号化アプライアンスとコンタクトします。
- [External URL]。受信者のメッセージは、この URL で IronPort 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、この URL でインバウンド HTTPS 要求を行います。

ステップ 6　[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。

- [High Security]。受信者は、暗号化されたメッセージを開封するには、パスワードを必ず入力する必要があります。
- [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。
- [No Password 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。受信者は、暗号化されたメッセージを開封するためにパスワードを入力する必要はありませんが、開封確認、安全な返信、安全な「全員に返信」、安全なメッセージ転送の機能は使用できず、別の電子メールのユーザが最初の受信者の代理でメッセージを送信することを防止できません。

ステップ 7　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。

- [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。
- [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 8　任意で、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 9　任意で、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、アプライアンスはメッセージをバウンスし、送信者に通知を送信します。

ステップ 10　任意で、暗号化アルゴリズムを選択します。

- [ARC4]。ARC4 は最もよく選択されるアルゴリズムで、メッセージ受信者に対する復号化遅延を最小限にとどめながら強力な暗号化を実現します。
- [AES]。AES は、より強力な暗号化を実現しますが、復号化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。

ステップ 11　復号化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 サーバで復号化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　[Message Settings] セクションで、[Secure Reply All] をイネーブルまたはディセーブルにします。

ステップ 13　[Secure Message Forwarding] をイネーブルまたはディセーブルにします。

ステップ 14　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。

（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。

ステップ 15　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。

ステップ 16　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、アプライアンスは通知を送信します。

ステップ 17　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 18　変更を送信して確定します。

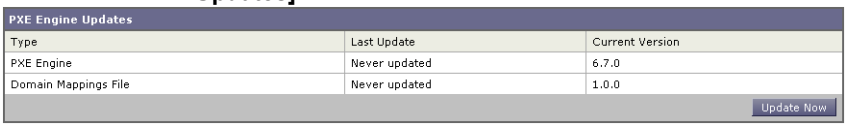
ステップ 19　Cisco Registered Envelope Service を使用する場合、アプライアンスをプロビジョニングする手順を追加で実行する必要があります。アプライアンスをプロビジョニングすると、暗号化プロファイルがホステッド キー サービスとともに登録されます。アプライアンスをプロビジョニングするには、登録する暗号化プロファイルの [Provision] ボタンをクリックします。

PXE エンジンの更新

[IronPort Email Encryption Settings] ページでは、PXE エンジンの現行バージョンとアプライアンスが使用するドメイン マッピング ファイルを表示します。AsyncOS の以前のバージョンでは、PXE エンジンを更新するには AsyncOS を更新する必要がありました。今では、[Security Services] > [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 IronPort アプライアンスを設定できます。詳細については、「サービスのアップデート」（P.15-486）を参照してください。

また、[IronPort Email Encryption Settings] ページの [PXE Engine Updates] セクションの [Update Now] ボタン（または CLI の `encryptionupdate` コマンド）を使って、手動でエンジンを更新することもできます。

図 12-4　[IronPort Email Encryption Settings] ページの [PXE Engine Updates]



暗号化コンテンツ フィルタの設定

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、IronPort 電子メール セキュリティ アプライアンス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。

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宛先制御に基づき、IronPort アプライアンスは TLS が使用可能であれば、メッセージを暗号化する代わりに TLS 接続でメッセージを中継します。アプライアンスは、宛先制御（Required、Preferred、または 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。表 12-2 では、暗号化制御フィルタが TLS 接続でのメッセージの送信を試みる場合、電子メール セキュリティ アプライアンスが、ドメインの宛先制御の 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 12-2　ESA アプライアンスの TLS サポート

宛先制御 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
[None]	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 Preferred]	TLS を通して送信します。	エンベロープを暗号化して送信します。
[TLS Required]	TLS を通して送信します。	リトライまたはメッセージのバウンス

宛先制御での TLS のイネーブル化の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章を参照してください。

Encrypt and Deliver Now コンテンツ フィルタの作成

メッセージを暗号化して即時に配信し、それ以降のプロセスをスキップするコンテンツ フィルタを作成するには、次の手順に従います。

ステップ 1　[Mail Policies] > [Outgoing Content Filters] に移動します。

ステップ 2　[Filters] セクションで、[Add Filter] をクリックします。

ステップ 3　[Conditions] セクションで、[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。

条件の作成の詳細については、「コンテンツ フィルタの概要」（P.6-198）を参照してください。

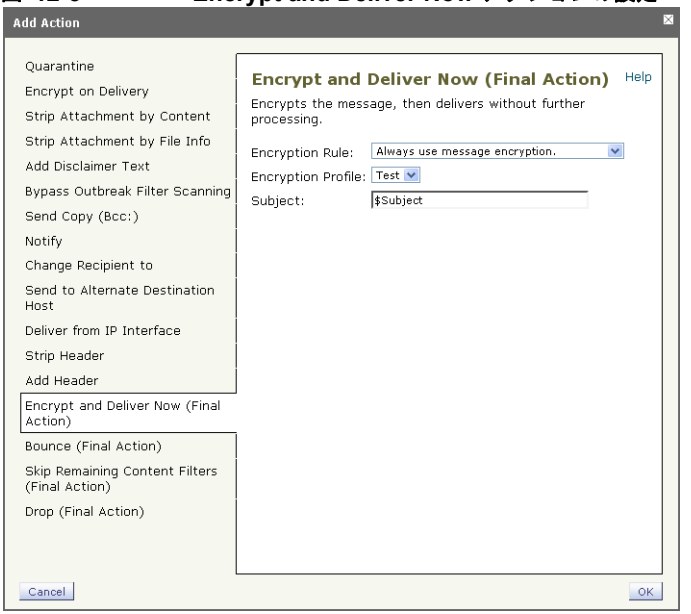
ステップ 6　任意で、[Add Action] をクリックし、[Add Header] を選択し、追加の暗号化設定を指定する暗号化ヘッダーをメッセージに挿入します。

暗号化ヘッダーの詳細については、「メッセージへの暗号化ヘッダーの追加」（P.12-412）を参照してください。

ステップ 7　[Actions] セクションで、[Add Action] をクリックします。

ステップ 8　[Encrypt and Deliver Now (Final Action)] を選択します。

図 12-5　Encrypt and Deliver Now アクションの設定



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。

図 12-6 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 12-6　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、[Submit] をクリックします。

ステップ 14　変更を確定します。

ステップ 15　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、「ユーザベース ポリシーの概要」（P.6-190）を参照してください。

Encrypt on Delivery コンテンツ フィルタの作成

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。

ステップ 1　[Mail Policies] > [Outgoing Content Filters] に移動します。

ステップ 2　[Filters] セクションで、[Add Filter] をクリックします。

ステップ 3　[Conditions] セクションで、[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。

条件の作成の詳細については、「コンテンツ フィルタの概要」（P.6-198）を参照してください。

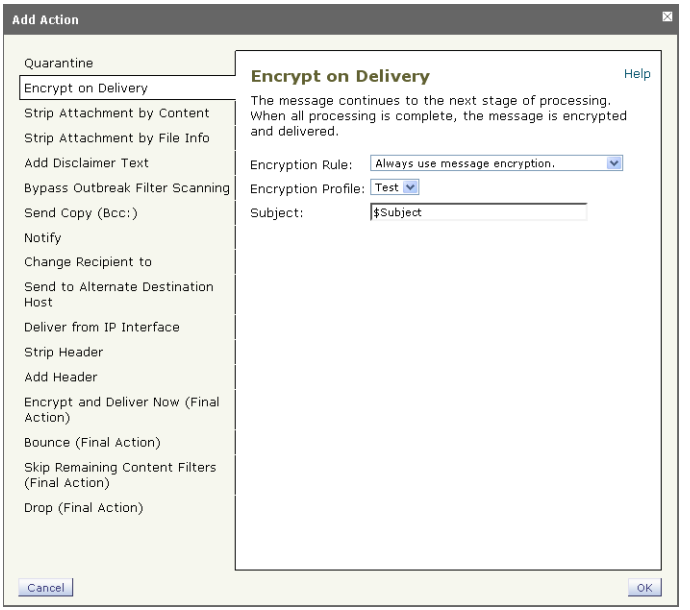
ステップ 6　任意で、[Add Action] をクリックし、[Add Header] を選択し、追加の暗号化設定を指定する暗号化ヘッダーをメッセージに挿入します。

暗号化ヘッダーの詳細については、「メッセージへの暗号化ヘッダーの追加」（P.12-412）を参照してください。

ステップ 7　[Actions] セクションで、[Add Action] をクリックします。

ステップ 8　[Encrypt on Delivery] を選択します。

図 12-7　Encrypt on Delivery アクションの設定



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、[Submit] をクリックします。

ステップ 14　変更を確定します。

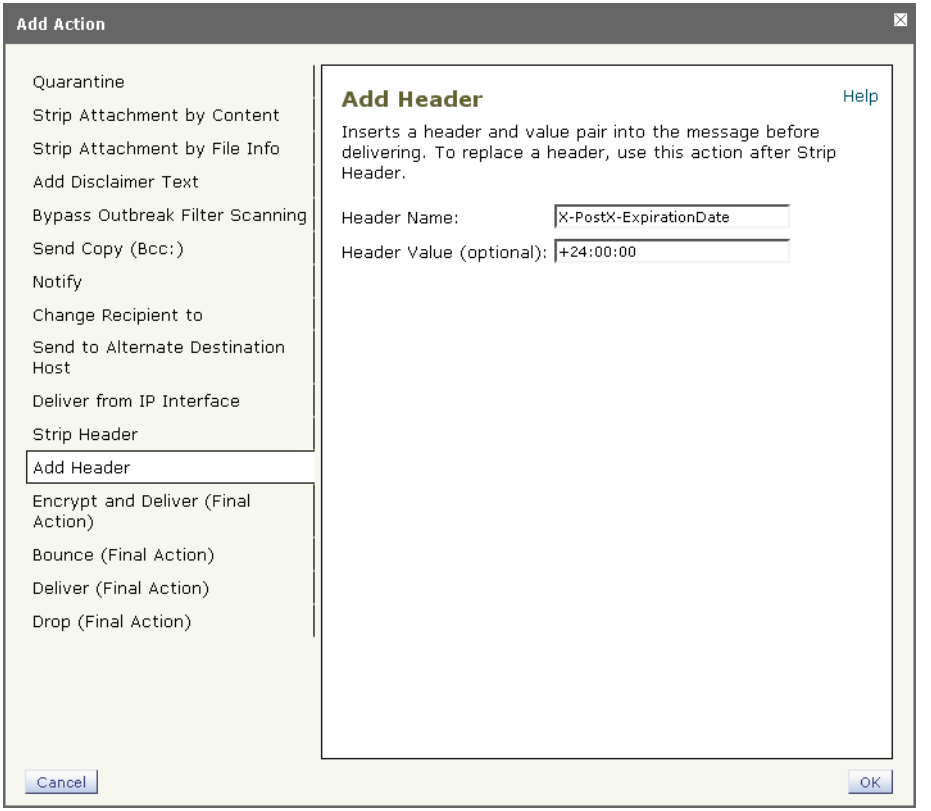
ステップ 15　コンテンツ フィルタを追加したら、フィルタを発信メール ポリシーに追加する必要があります。組織のニーズに応じて、デフォルト ポリシーでコンテンツ フィルタをイネーブルにする、またはフィルタを特定のメール ポリシーに適用することを選択します。メール ポリシーの操作については、「ユーザベース ポリシーの概要」（P.6-190）を参照してください。

メッセージへの暗号化ヘッダーの追加

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。

コンテンツ フィルタを使って暗号化ヘッダーをメッセージに追加するには、Add Header フィルタ アクションをコンテンツ フィルタに追加し、暗号化ヘッダーとその値を入力します。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。

図 12-8　Add Header アクションの設定



暗号化コンテンツ フィルタの作成の詳細については、「Encrypt and Deliver Now コンテンツ フィルタの作成」（P.12-407）を参照してください。メッセージ フィルタを使ったヘッダーの挿入については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章を参照してください。

暗号化ヘッダー

表 12-3 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 12-3　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 [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。	[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 false 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 [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。	[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 false です。
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 [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。	[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 false 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 false です。

表 12-3　電子メール暗号化ヘッダー（続き）

MIME ヘッダー	説明	値
X-PostX-ExpirationDate	送信前に Registered Envelope の有効期限の日付けを設定します。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-ReadNotificationDate	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。

表 12-3　電子メール暗号化ヘッダー（続き）

MIME ヘッダー	説明	値
X-PostX-Suppress-Applet-For-Open	復号化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。復号化アプレットにより、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 サーバで復号化されます。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。	復号化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 false です。

表 12-3　電子メール暗号化ヘッダー（続き）

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ワードを入力し、[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化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ワード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、[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 false 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。

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
```

[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をイネーブルにする

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 Open Online リンクとともに表示され、[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をイネーブルにする

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。

復号化アプレットをディセーブルにする

復号化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）　復号化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。