メール ポリシーとコンテンツ フィルタの例

この付録は、次のセクションで構成されています。

受信メール ポリシーの概要

この例では、次のタスクを示し、メール ポリシーの機能について説明します。

1. デフォルトの着信メールポリシーのアンチスパム、アンチウイルス、アウトブレイク フィルタおよびコンテンツ フィルタを編集します。
2. 販売部とエンジニアリング部の異なるユーザのセットに 2 つの新しいポリシーを追加して、それぞれに異なる電子メール セキュリティ設定を指定します。
3. [着信メール ポリシーの概要（Incoming Mail Overview policy）] テーブルで使用する 3 つの新しいコンテンツ フィルタを作成します。
4. ポリシーをもう一度編集して、コンテンツ フィルタをグループによってイネーブルまたはディセーブルにします。

この例では、受信者によって異なるメールポリシーのアンチスパム、アンチウイルス、アウトブレイク フィルタおよびコンテンツ フィルタの設定を管理できる、機能と柔軟性を示しています。この例では、メール ポリシーおよびコンテンツ フィルタのアクセス権限を持つ「ポリシー管理者」と呼ばれるカスタム ユーザー ロールを割り当てます。アンチスパム、アンチウイルス、アウトブレイク フィルタ、および委任管理の機能の詳細については、次の章を参照してください。

- スパムおよびグレイメールの管理
- アンチウイルス
- アウトブレイク フィルタ
- 管理タスクの分散

メール ポリシーへのアクセス

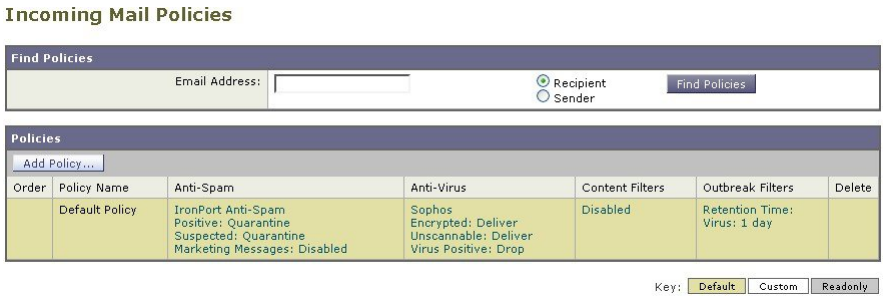
[メールポリシー（Mail Policies）] メニューを使用して、着信および発信メール ポリシーにアクセスできます。

新規システムでは、システムセットアップ ウィザードのすべての手順を完了して、Anti-Spam、Sophos または McAfee Anti-Virus およびアウトブレイク フィルタをイネーブルにするように選択した場合、以下の図のような [着信メールポリシー（Incoming Mail Policies）] ページが表示されます。

デフォルトでは、これらの設定は、デフォルトの着信メール ポリシーでイネーブルにされます。

- アンチスパム（ スパム隔離がイネーブルの場合）：イネーブル
  - 陽性と判定されたスパム：隔離、メッセージの件名が追加
  - 陽性と疑わしいスパム：隔離、メッセージの件名が追加
  - マーケティング電子メール：スキャンはイネーブルにされない
- アンチスパム（スパム隔離がイネーブルではない場合）：イネーブル
  - 陽性と判定されたスパム：配信、メッセージの件名が追加
  - 陽性と疑わしいスパム：配信、メッセージの件名が追加
  - マーケティング電子メール：スキャンはイネーブルにされない
- アンチウイルス：イネーブル、ウイルスのスキャンおよび修復、アンチウイルス スキャン結果が X-Header に追加
  - 修復されたメッセージ：配信、メッセージの件名が追加
  - 暗号化されたメッセージ：配信、メッセージの件名が追加
  - スキャンできないメッセージ：配信、メッセージの件名が追加
  - ウイルスに感染したメッセージ：ドロップ
- アウトブレイク フィルタ：イネーブル
  - ファイル拡張子は予測されない
  - 疑わしいウイルス添付ファイルのあるメッセージの保存期間は 1 日
  - メッセージの変更は有効ではない
- コンテンツ フィルタ：ディセーブル

図 *1 : [*着信メールポリシー（***Incoming Mail Policies***）*]* ページ：新規アプライアンスのデフォルト



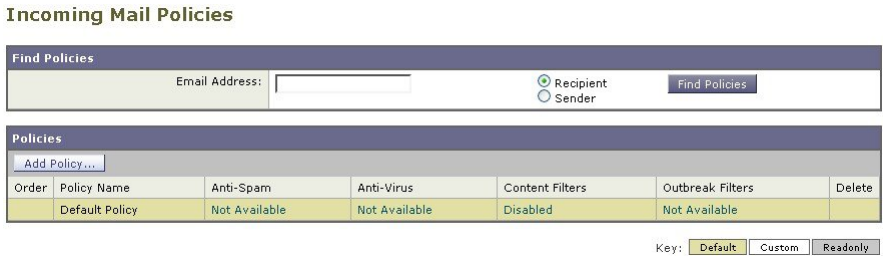
（注） この例では、着信メールポリシーは、スパム隔離がイネーブルにされている場合のデフォルトのアンチスパム設定を使用します。

[有効（Enabled）]、[無効（Disabled）]、[利用不可（Not Available）]

メールポリシーテーブル（着信または発信のいずれか）の列は、各ポリシー名のセキュリティサービスの状態のリンクを表示します。サービスがイネーブルの場合、[有効（Enabled）] という語またはコンフィギュレーションの要約が表示されます。同様に、サービスがディセーブルの場合、[無効（Disabled）] という語が表示されます。

サービスのライセンス契約書に同意していない場合、またはサービスの有効期限が切れている場合、リンクとして [利用不可（Not Available）] が表示されます。この場合、[利用不可（Not Available）] リンクをクリックすると、[セキュリティ サービス（Security Services）] タブ内に、サービスのポリシー単位の設定を指定できるページではなく、グローバルページが表示されます。ページが別のタブに変わったことを示す警告が表示されます。次の図を参照してください。

図 *2 :* 使用できないセキュリティ サービス



着信メッセージのデフォルトのアンチスパム ポリシーの設定

このメールポリシーテーブル内の各行は、異なるポリシーを表します。各列は、異なるセキュリティ サービスを表します。

- デフォルト ポリシーを編集するには、着信または発信メール ポリシー テーブルの下部の行にあるセキュリティ サービスの任意のリンクをクリックします。

メール ポリシーとコンテンツ フィルタの例

この例では、着信メールのデフォルト ポリシーのアンチスパム設定をより積極的に変更します。デフォルト値では、陽性と判定されたスパム メッセージおよび陽性と疑わしいスパム メッセージが隔離され、マーケティング電子メールのスキャンがディセーブルになります。次に、陽性と判定されたスパムがドロップされるように設定を変更する例を示します。陽性と疑わしいスパムは引き続き隔離されます。マーケティング電子メールのスキャンは、イネーブルにされ、マーケティング メッセージは目的の受信者に配信されます。マーケティング メッセージの件名には、テキスト [MARKETING] が前に追加されます。

手順

ステップ 1 アンチスパム セキュリティ サービスのリンクをクリックします。

（注） デフォルトのセキュリティ サービス設定の場合、このページの最初の設定では、ポリシーでサービスがイネーブルになるかどうかを定義します。[無効（Disable）] をクリックしてすべてのサービスをディセーブルにできます。

ステップ 2 [陽性と判定されたスパムの設定（Positively Identified Spam Settings）] セクションでは、[このメッセージに適用されるアクション（Action to apply to this message）] を [ドロップ（Drop）] に変更します。

ステップ 3 [マーケティングメールの設定（Marketing Email Settings）] セクションでは、[はい（Yes）] をクリックして、マーケティング電子メールのスキャンをイネーブルにします。

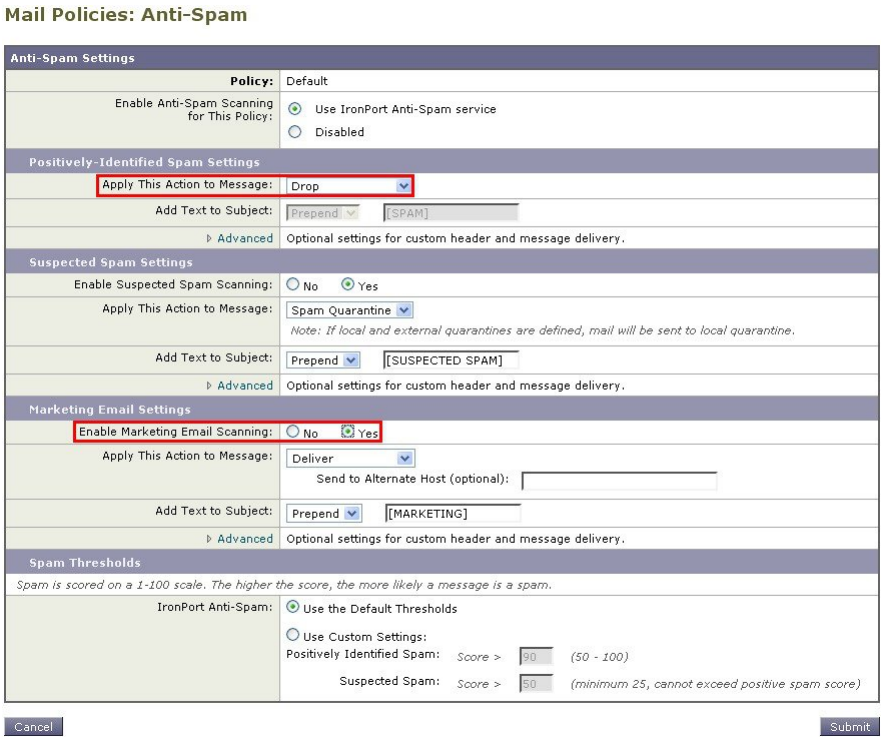
イネーブルにされている場合、デフォルト アクションでは、テキスト [MARKETING] が件名の前に追加され、問題のないマーケティング メッセージが配信されます。

[メッセージにテキストを追加（Add text to message）] フィールドでは、US-ASCII 文字だけを使用できます。

ステップ 4 [送信（Submit）] をクリックします。着信メール ポリシー テーブルのアンチスパム セキュリティ サービスの要約リンクが変更され、新しい値が反映されているため注意してください。

前述の手順と同様、デフォルト ポリシーのデフォルト アンチウイルスおよびウイルス アウトブレイク フィルタ設定を変更できます。

図 *3 : [*スパム対策設定（***Anti-Spam Settings***）*]* ページ



送信者および受信者のグループのメール ポリシーの作成

この例では、販売部（メンバーはLDAP受け入れクエリーにより定義されます）用とエンジニアリング部用の2つの新しいポリシーを作成します。ポリシーは両方とも、これらのポリシーの管理を担当するロールに属す委任管理者を作成するためにポリシー管理者カスタム ユーザ ロールに割り当てられます。次に、それぞれに異なる電子メールセキュリティ設定を設定します。

手順

ステップ 1 [ポリシーを追加（Add Policy）]ボタンをクリックして、新しいポリシーの作成を開始します。

ステップ 2 一意な名前を定義して、（必要な場合）ポリシーの順序を調整します。

ポリシーの名前は、定義されるメール ポリシー テーブル（着信または発信のいずれか）で一意でなければなりません。

各受信者は、適切なテーブル（着信または発信）の各ポリシーに対して上から順に評価されます。

メール ポリシーとコンテンツ フィルタの例

ステップ 3 [編集可能なユーザ（役割）（Editable By (Roles)）] リンクをクリックし、メール ポリシーの管理を担当する委任管理者にカスタム ユーザ ロールを選択します。

リンクをクリックすると、AsyncOS は、メール ポリシーの編集権限がある委任管理者のカスタム ロールを表示します。委任管理者は、ポリシーのアンチスパム、アンチウイルス、アウトブレイク フィルタの設定を編集し、ポリシーのコンテンツ フィルタを有効化または無効化できます。オペレータおよび管理者のみがメール ポリシーの名前または送信者、受信者、またはグループを変更できます。メール ポリシーへのフル アクセス権があるカスタム ユーザ ロールはメール ポリシーに自動的に割り当てられます。

委任管理の詳細については、管理タスクの分散を参照してください。

ステップ 4 ポリシーのユーザを定義します。

ユーザが、送信者または受信者のいずれであるかを定義します（詳細については、ポリシー マッチングの例を参照してください）。以下の図では、着信メール ポリシーの受信者および発信メール ポリシーの送信者というデフォルト形式を示しています。

ポリシーのユーザは、次の方法で定義できます。

- 完全な電子メール アドレス：user@example.com
- 電子メール アドレスの一部：user@
- ドメインのすべてのユーザ：@example.com
- 部分ドメインのすべてのユーザ：@.example.com
- LDAP クエリーとのマッチング

（注） ユーザの入力は、AsyncOS の GUI および CLI の両方で、大文字と小文字が区別されます。たとえば、ユーザの受信者 Joe@ を入力すると、joe@example.com に送信されるメッセージが一致します。

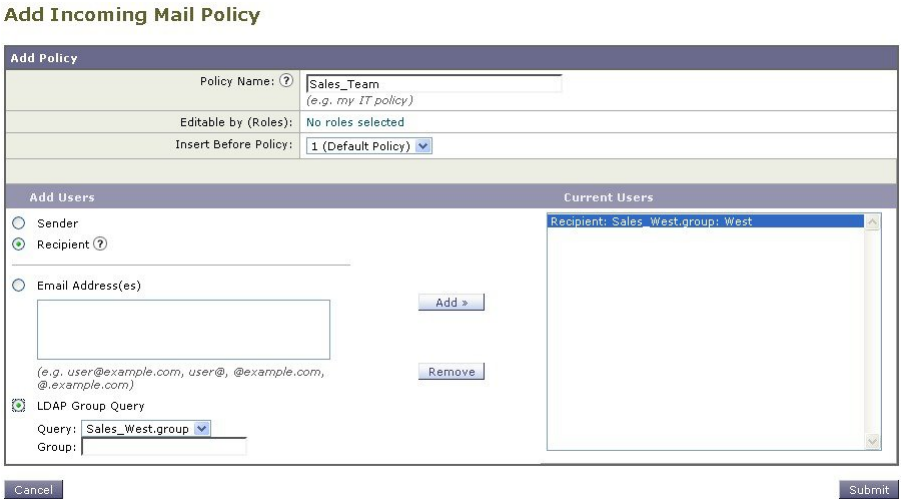
ユーザ情報を、たとえば Microsoft Active Directory、SunONE Directory Server（以前の「iPlanet Directory Server」）または Open LDAP ディレクトリなど、ネットワーク インフラストラクチャの LDAP ディレクトリ内に保存する場合、アプライアンスを設定して、LDAP サーバをクエリし、受信者アドレスの受け取り、代替アドレスまたはメールホスト、あるいはその両方へのメッセージのリルーティング、ヘッダーのマスカレード、メッセージに特定のグループの受信者または送信者があるかどうかの判別を行うことができます。

アプライアンスをこのように設定した場合、設定したクエリーを使用してメールポリシーのユーザを定義できます。

詳細については、LDAP クエリを参照してください。

メール ポリシーとコンテンツ フィルタの例

図 *4*：ポリシーのユーザの定義



ステップ 5 [追加（Add）]ボタンをクリックして、[現在のユーザ（Current Users）]リストにユーザを追加します。

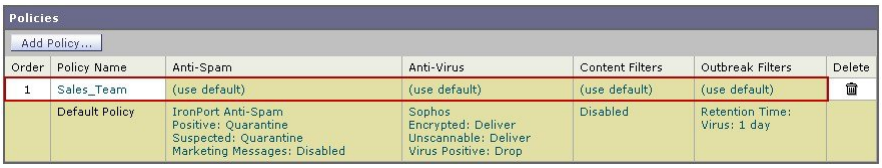
ポリシーには、送信者、受信者およびLDAPクエリーを組み合わせて含めることができます。

[削除（Remove）]ボタンを使用すると、定義されているユーザを現在のユーザのリストから削除できます。

ステップ 6 ユーザの追加が完了したら、[送信（Submit）] をクリックします。

ポリシーを最初に追加する場合、すべてのセキュリティ サービス設定では、デフォルト値が使用されるため注意してください。

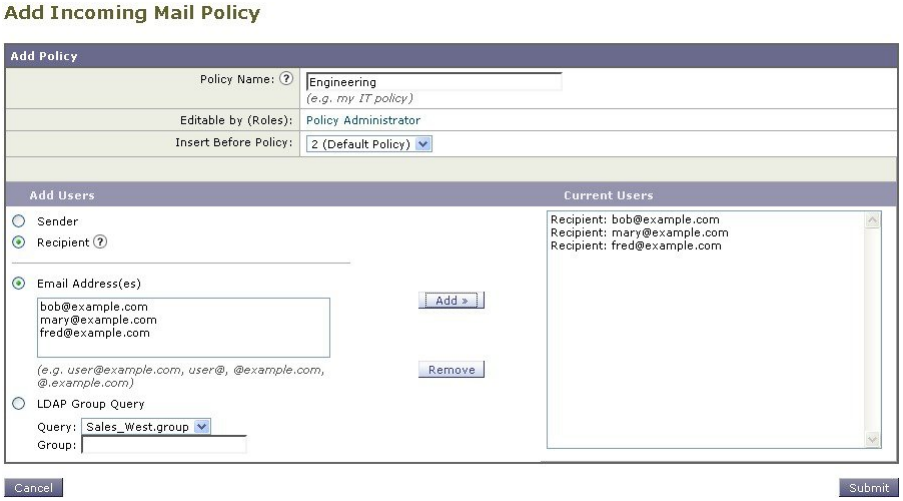
図 *5*：新しく追加されたポリシー：販売グループ



ステップ 7 [ポリシーを追加（Add Policy）] ボタンをもう一度クリックして、別の新しいポリシーを追加します。

このポリシーでは、エンジニアリング チームのメンバーの各電子メール アドレスが定義されます。

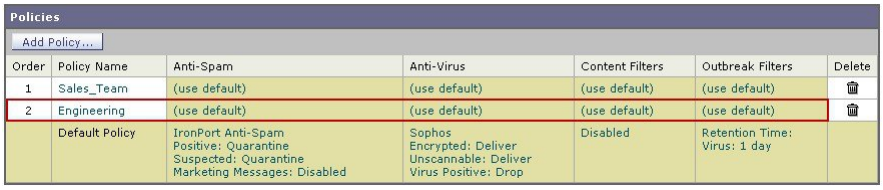
図 *6:* エンジニアリング チームのポリシーの作成



ステップ 8 エンジニアリング ポリシーのユーザの追加が完了したら、[送信（Submit）] をクリックします。

ステップ 9 変更を保存します。

図 *7:* 新しく追加されたポリシー：エンジニアリング チーム



（注） この時点では、新しく作成された両方のポリシーに、デフォルト ポリシーで使用される同じ設定が適用されています。いずれかのポリシーのユーザへのメッセージが一致しますが、メール処理設定は、デフォルト ポリシーと同じです。そのため、「Sales_Group」または「Engineering」ポリシーのユーザと一致するメッセージは、デフォルト ポリシーと同様に処理されます。

[デフォルト（Default）]、[カスタム（Custom）]、[無効（Disabled）]

テーブル下部のキーは、特定のポリシーのセルのカラー コーディングが、デフォルト行に定義されているポリシーとどのように関係するかを示しています。

- イエローのシェーディングは、ポリシーがデフォルト ポリシーと同じ設定を使用していることを示します。
- シェーディングなし（ホワイト）は、ポリシーがデフォルト ポリシーとは異なる設定を使用していることを示します。
- グレーのシェーディングは、セキュリティ サービスがポリシーでディセーブルにされていることを示します。

送信者および受信者のグループごとのメール ポリシーの作成

この例では、前述の項で作成した 2 つのポリシーを編集します。

- 販売グループでは、アンチスパム設定をデフォルト ポリシーよりも積極的になるように変更します（着信メッセージのデフォルトのアンチスパム ポリシーの設定 （3 ページ） を参照。）陽性と識別されたスパム メッセージをドロップするデフォルト ポリシーが使用されます。ただし、この例では、スパム隔離エリアに送信されるように、マーケティング メッセージの設定を変更します。

  この積極的なポリシーでは、販売チームの受信トレイに送信される不要なメッセージが最小限に押さえられます。

  アンチスパム設定の詳細については、スパムおよびグレイメールの管理を参照してください。

- エンジニアリング チームでは、example.com へのリンクを除く疑わしいメッセージの URL を変更するために、アウトブレイク フィルタ機能の設定をカスタマイズします。拡張子「dwg」の添付ファイルは、アウトブレイク フィルタのスキャンをバイパスします。

  アウトブレイク フィルタの設定の詳細については、アウトブレイク フィルタを参照してください。

  販売チーム ポリシーのアンチスパム設定を編集するには、次の手順を実行します。

手順

ステップ 1 販売ポリシー行のアンチスパム セキュリティ サービス（[スパム対策（Anti-Spam）]）列のリンクをクリックします。

このポリシーは新しく追加されたポリシーであるため、リンクの名前は[（デフォルトを使用）（use default）] です。

ステップ 2 アンチスパム セキュリティ サービス ページで、[このポリシーのスパム対策スキャンを有効にする（Enable Anti-Spam Scanning for this Policy）] の値を [デフォルト設定を使用（Use Default Settings）] から [スパム対策を使用（Use Cisco Anti-Spam）] に変更します。

[スパム対策サービスを使用（Use Cisco Anti-Spam service）] を選択すると、デフォルト ポリシーで定義されている設定が無効になります。

ステップ 3 [スパムと確定された場合の設定（Positively-Identified Spam Settings）] セクションで、[このアクションをメッセージに適用する（Apply This Action to Message）] を [ドロップ（Drop）] に変更します。

ステップ 4 [疑わしいスパムの設定（Suspected Spam Settings）] セクションで、[はい（Yes）] をクリックして、陽性と疑わしいスパムのスキャンをイネーブルにします。

ステップ 5 [疑わしいスパムの設定（Suspected Spam Settings）] セクションで、[このアクションをメッセージに適用する（Apply This Action to Message）] を [スパム隔離（Spam Quarantine）] に変更します。

（注） [スパム隔離（Spam Quarantine）] を選択すると、「スパム隔離」の章で定義されている設定に従って、メールが転送されます。

ステップ 6 [件名へテキストを追加（Add text to subject）] フィールドで、[なし（None）] をクリックします。

スパム隔離エリアに配信されるメッセージには、件名タギングが追加されません。

ステップ 7 [マーケティングメールの設定（Marketing Email Settings）] セクションで、[はい（Yes）] をクリックして、問題のない送信元からのマーケティング メールのスキャンをイネーブルにします。

ステップ 8 [このアクションをメッセージに適用する（Apply This Action to Message）] セクションで、[スパム隔離（Spam Quarantine）] を選択します。

ステップ 9 変更を送信し、保存します。

このシェーディングは、ポリシーがデフォルトポリシーとは異なる設定を使用していることを示します。

この時点では、スパムの疑いがあり、その受信者が販売チーム ポリシーで定義されている LDAP クエリーと一致するメッセージは、IronPort スパム検疫エリアに配信されます。

送信者および受信者のグループごとのメール ポリシーの作成

エンジニアリング チーム ポリシーのアウトブレイク フィルタ設定を編集するには、次の手順を実行します。

手順

ステップ 1 エンジニアリング ポリシー行のアウトブレイク フィルタ機能セキュリティ サービス（[アウトブレイクフィルタ（Outbreak Filters）] カラム）のリンクをクリックします。

このポリシーは新しく追加されたポリシーであるため、リンクの名前は[（デフォルトを使用）（use default）] です。

ステップ 2 [アウトブレイク フィルタ機能セキュリティ サービス（Outbreak Filters feature security service）] ページで、ポリシーのスキャン設定を [アウトブレイクフィルタを有効にする（設定をカスタマイズ）（Enable Outbreak Filtering (Customize settings)）] に変更します。

[（設定をカスタマイズ）（(Customize settings)）] を選択すると、デフォルト ポリシーで定義されている設定が無効になります。

また、別の設定を選択できるようにページの残りの部分のコンテンツがイネーブルになります。

ステップ 3 ページの [添付ファイルのスキャンのバイパス（Bypass Attachment Scanning）] セクションで、ファイル拡張子フィールドに **dwg** と入力します。

メール ポリシーとコンテンツ フィルタの例

ファイル拡張子「dwg」は、アプライアンスが添付ファイルのスキャン時にフィンガープリントにより認識できる既知のファイルタイプのリストにはありません。

（注） 3 文字のファイル拡張子の前にピリオド（.）を入力する必要はありません。

ステップ 4 [拡張子を追加（Add Extension）] をクリックして、.dwg ファイルをアウトブレイク フィルタ機能スキャンをバイパスするファイル拡張子のリストに追加します。

ステップ 5 [メッセージの変更を有効にする（Enable Message Modification）] をクリックします。

メッセージの変更を有効にすると、アプライアンスはフィッシングおよび詐欺など脅威としてターゲットされるものや、疑わしいまたは不正な Web サイトへの URL がスキャンできるようになります。アプライアンスは、ユーザが Web サイトへアクセスしようとすると Cisco セキュリティプロキシを介してリダイレクトするように、メッセージ中のリンクを書き換えます。

（注） アウトブレイク フィルタが非ウイルス性の脅威をスキャンするために、メール ポリシーでアンチスパム スキャンをイネーブルにする必要があります。

ステップ 6 [未署名のメッセージに対して有効にする（Enable for Unsigned Messages）] を選択します。

その結果、アプライアンスは署名されたメッセージの URL を書き変えることができます。他のメッセージの変更および非ウイルス性の脅威が検出されたメッセージが解放されるまで隔離にとどまる時間が設定ができるように URL の書き換えをイネーブルにする必要があります。この例では、デフォルトの保存期間は 4 時間です。

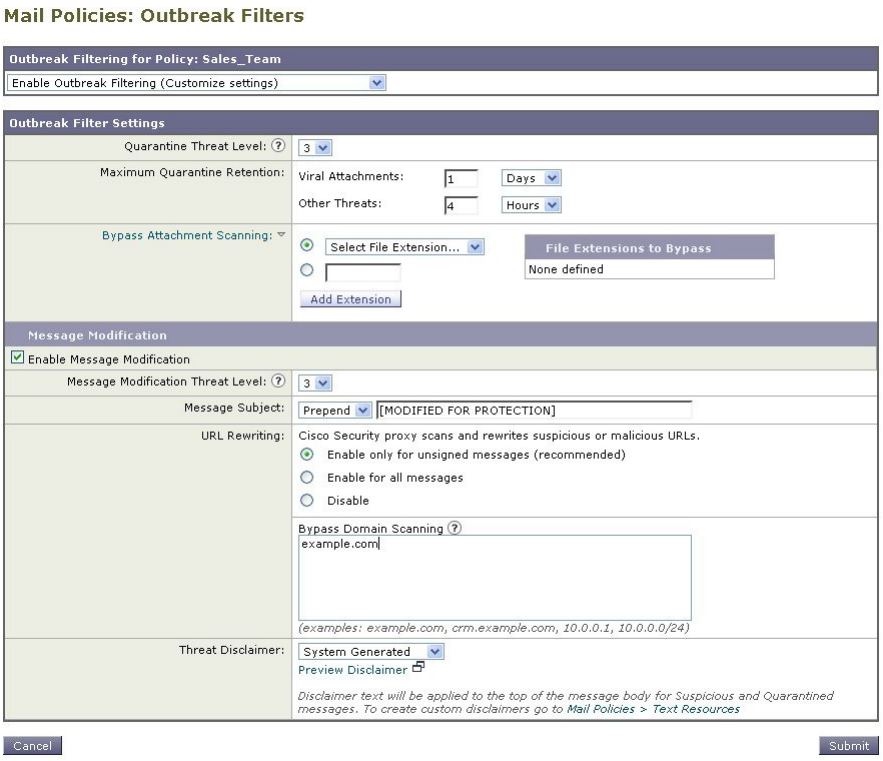
ステップ 7 [ドメインのスキャンをバイパス（Bypass Domain Scanning）] フィールドに example.com と入力します。

アプライアンスは example.com へのリンクを変更しません。

ステップ 8 [脅威に関する免責事項（Threat Disclaimer）] で [システムが生成（System Generated）] を選択します。

アプライアンスは、メッセージの内容についてユーザに警告するためにメッセージ本文の上に免責事項を挿入できます。次の例では、システムで生成された脅威に関する免責事項を使用しています。

図 *8:* アウトブレイク フィルタの設定



ステップ 9 変更を送信し、保存します。

このシェーディングは、ポリシーがデフォルト ポリシーとは異なる設定を使用していることを示します。

この時点では、ファイル拡張子が dwg である添付ファイルを含む任意のメッセージ、および受信者がエンジニアリング チーム ポリシーで定義されている受信者とマッチングする任意のメッセージは、アウトブレイク フィルタ スキャンをバイパスし、処理を続行します。example.com ドメインへのリンクを含むメッセージは、Cisco セキュリティ プロキシを介してリダイレクトするようにリンクを修正されることはなく、疑わしいと見なされません。

メール ポリシーでの送信者または受信者の検索

[ポリシー検索（Find Policies）] ボタンを使用して、[受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（Outgoing Mail Policies）] ページで定義されているポリシーですでに定義されているユーザを検索します。

たとえば、joe@example.com と入力して、[ポリシー検索（Find Policies）] ボタンをクリックすると、ポリシーとマッチングする特定の定義済みユーザを含むポリシーを示す結果が表示されます。

ポリシーの名前をクリックして、[ポリシー設定を編集（Edit Policy）] ページに移動してそのポリシーのユーザを編集します。

ユーザを検索する場合、デフォルト ポリシーは常に表示されるため注意してください。これは、定義上、送信者または受信者が設定されているポリシーと一致しない場合、デフォルトのポリシーが必ず一致するためです。

管理例外

前述の2つの例で示されている手順を使用して、管理例外に基づいたポリシーの作成および設定を開始できます。つまり、組織のニーズを評価した後で、メッセージの大部分がデフォルトポリシーで処理されるように、ポリシーを設定できます。また、必要に応じて、異なるポリシーを管理して、特定のユーザまたはユーザ グループの追加「例外」ポリシーを作成できます。このようにすることで、メッセージ分裂が最小化され、ワーク キューの各分裂メッセージの処理により受けるシステム パフォーマンスの影響が少なくなります。

スパム、ウイルスおよびポリシー実行に対する組織またはユーザの許容値に基づいて、ポリシーを定義できます。次の表に、いくつかのポリシーの例の概要を示します。「積極的な」ポリシーでは、エンドユーザのメールボックスに到達するスパムおよびウイルスの量が最小限に抑えられます。「保守的な」ポリシーでは、偽陽性を回避し、ポリシーに関係なく、ユーザによるメッセージの見落としを防ぐことができます。

表 *1*：積極的および保守的なメール ポリシーの設定

	積極的な設定	保守的な設定
スパム対策	陽性と判定されたスパム：ドロップ 陽性と疑わしいスパム：隔離 マーケティング メール：メッセージの件名の前に「[Marketing]」が追加されて配信	陽性と判定されたスパム：隔離 陽性と疑わしいスパム：メッセージの件名の前に「[Suspected Spam]」が追加されて配信 マーケティング メール：ディセーブル
ウイルス対策	修復されたメッセージ：配信 暗号化されたメッセージ：ドロップ スキャンできないメッセージ：ドロップ 感染メッセージ：ドロップ	修復されたメッセージ：配信 暗号化されたメッセージ：隔離 スキャンできないメッセージ：隔離 感染メッセージ：ドロップ
ウイルス フィルタ	イネーブル、バイパスできる特定のファイル名拡張子またはドメインなし すべてのメッセージのメッセージ変更の有効化	バイパスできるファイル名拡張子またはドメインの有効化 未署名のメッセージのメッセージ変更の有効化

コンテンツに基づくメッセージのフィルタリング

この例では、[受信メールポリシー（Incoming Mail Policy）] テーブルで使用される新しいコンテンツ フィルタを 3 つ作成します。これらのコンテンツ フィルタは、ポリシー管理のカスタム ユーザー ロールに属す委任管理者が編集できます。次のフィルタを作成します。

1. 「scan_for_confidential」

   このフィルタは、文字列「confidential」が含まれているかメッセージをスキャンします。文字列が見つかると、メッセージのコピーが電子メール エイリアス hr@example.com に送信され、メッセージがポリシー隔離エリアに送信されます。

2. 「no_mp3s」

   このフィルタは、MP3 添付ファイルを削除し、MP3 ファイルが削除されたことを受信者に通知します。

3. 「ex_employee」

   このコンテンツ フィルタは、特定のエンベロープ受信者アドレス（元受信者）に送信されるメッセージをスキャンします。メッセージが一致した場合、特定の通知メッセージがメッセージ送信者に送信され、メッセージがバウンスされます。

コンテンツ フィルタを作成したら、各ポリシー（デフォルト ポリシーを含む）を設定して、異なる組み合わせで特定のコンテンツ フィルタをイネーブルにします。

件名に「Confidential」とあるメッセージの隔離

最初の例のコンテンツ フィルタには、1 つの条件と 2 つのアクションが含まれます。

手順

ステップ 1 [メールポリシー（Mail Policies）] タブをクリックします。

ステップ 2 [受信コンテンツフィルタ（Incoming Content Filters）] をクリックします。

ステップ 3 [フィルタを追加（Add Filter）] ボタンをクリックします。

ステップ 4 [名前（Name）] フィールドに、新しいフィルタの名前として scan_for_confidential と入力します。

フィルタ名には、ASCII 文字、数字、下線またはダッシュを含めることができます。コンテンツ フィルタ名の最初の文字は、文字または下線でなければなりません。

ステップ 5 [編集可能なユーザ（役割）（Editable By (Roles)）] リンクをクリックし、[ポリシー管理者（Policy Administrator）] を選択し、[OK] をクリックします。

ポリシー管理者ユーザ ロールに属する委任管理者はこのコンテンツ フィルタを編集し、自身のメール ポリシーで使用できます。

ステップ 6 [説明（Description）] フィールドに、説明を入力します。たとえば、「scan all incoming mail for the string ‘confidential’」と入力します。

ステップ 7 [条件を追加（Add Condition）] をクリックします。

ステップ 8 [メッセージ本文（Message Body）] を選択します。

ステップ 9 [テキストを含む:（Contains text:）] フィールドに confidential と入力して、[OK] をクリックします。

[コンテンツフィルタの追加（Add Content Filter）] ページに、追加される条件が表示されます。

ステップ 10 [アクションを追加（Add Action）] をクリックします。

ステップ 11 [コピーを送信(Bcc:)（Send Copy To (Bcc:)）] を選択します。

ステップ 12 [メールアドレス（Email Addresses）] フィールドに、hr@example.com と入力します。

ステップ 13 [件名（Subject）] フィールドに、[message matched confidential filter] と入力します。

ステップ 14 [OK] をクリックします。

[コンテンツフィルタの追加（Add Content Filter）] ページに、追加されるアクションが表示されます。

ステップ 15 [アクションを追加（Add Action）] をクリックします。

ステップ 16 [隔離（Quarantine）] を選択します。

ステップ 17 ドロップダウン メニューで、[ポリシー隔離領域（Policy quarantine area）] を選択します。

ステップ 18 [OK] をクリックします。

[コンテンツフィルタの追加（Add Content Filter）] ページに、追加される 2 番目のアクションが表示されます。

ステップ 19 変更を送信し、保存します。

この時点では、コンテンツフィルタは、いずれの着信メールポリシーでも有効になっていません。この例では、新しいコンテンツフィルタをプライマリリストに追加しただけの状態です。このコンテンツフィルタはいずれのポリシーにも適用されていないため、アプライアンスによる電子メール処理は、このフィルタの影響を受けません。

メッセージから MP3 添付ファイルを除去

2 番目の例のコンテンツ フィルタには、条件はなく、アクションは 1 つ含まれます。

手順

ステップ 1 [フィルタを追加（Add Filter）] ボタンをクリックします。

ステップ 2 [名前（Name）] フィールドに、新しいフィルタの名前として no_mp3s と入力します。

ステップ 3 [編集可能なユーザ（役割）（Editable By (Roles)）] リンクをクリックし、[ポリシー管理者（Policy Administrator）] を選択し、[OK] をクリックします。

ステップ 4 [説明（Description）] フィールドに、説明を入力します。たとえば、strip all MP3 attachments と入力します。

ステップ 5 [アクションを追加（Add Action）] をクリックします。

ステップ 6 [ファイル情報によって添付ファイルを除去（Strip Attachment by File Info）] を選択します。

ステップ 7 [ファイルタイプが次の場合（File type is）] を選択します。

ステップ 8 ドロップダウン フィールドで、[-- mp3] を選択します。

ステップ 9 必要な場合、置換メッセージを入力します。

ステップ 10 [OK] をクリックします。

ステップ 11 変更を送信し、保存します。

（注） コンテンツ フィルタを作成するときに条件を指定する必要はありません。条件が定義されていない場合、定義されるアクションは常にルールに適用されます（条件を指定しないことは、true() メッセージ フィルタ ルールを使用すること同じで、コンテンツ フィルタがポリシーに適用される場合、すべてのメッセージがマッチングされます）。

元従業員に送られたバウンス メッセージ

3 番目の例のコンテンツ フィルタには、1 つの条件と 2 つのアクションを使用します。

手順

ステップ 1 [フィルタを追加（Add Filter）] ボタンをクリックします。

ステップ 2 [名前:（Name:）] フィールドに、新しいフィルタの名前として **ex_employee** と入力します。

ステップ 3 [編集可能なユーザ（役割）（Editable By (Roles)）] リンクをクリックし、[ポリシー管理者（Policy Administrator）] を選択し、[OK] をクリックします。

ステップ 4 [説明：（Description:）] フィールドに、説明を入力します。たとえば、**bounce messages intended for Doug** と入力します。

ステップ 5 [条件を追加（Add Condition）] をクリックします。

ステップ 6 [エンベロープ受信者（Envelope Recipient）] を選択します。

ステップ 7 エンベロープ受信者に対して、[次で始まる（Begins with）] を選択して、**doug@** と入力します。

ステップ 8 [OK] をクリックします。

[コンテンツフィルタ（Content Filters）] ページがリフレッシュされ、追加された条件が表示されます。元従業員の電子メール アドレスを含む LDAP ディレクトリを作成できます。元従業員がそのディレクトリに追加されると、このコンテンツ フィルタは、動的に更新されます。

ステップ 9 [アクションを追加（Add Action）] をクリックします。

ステップ 10 [通知（Notify）] を選択します。

ステップ 11 [送信者（Sender）] チェックボックスを選択して、[件名（Subject）] フィールドに、 message bounced for ex-employee of **example.com** と入力します。

ステップ 12 [テンプレート利用（Use template）] セクションで、通知テンプレートを選択します。

（注） リソースが事前に定義されていないため、コンテンツ フィルタ ルール ビルダのいくつかのセクションは、ユーザーインターフェイスに表示されません。たとえば、コンテンツディクショナリ、通知テンプレートおよびメッセージ免責事項は、[メールポリシー（Mail Policies）]>[ディクショナリ（Dictionaries）]ページ（またはCLIの**dictionaryconfig**コマンド）から事前に設定されていない場合、オプションとして表示されません。ディクショナリの作成の詳細については、コンテンツディクショナリを参照してください。

ステップ 13 [OK] をクリックします。

[コンテンツフィルタの追加（Add Content Filters）] ページに、追加されるアクションが表示されます。

ステップ 14 [アクションを追加（Add Action）] をクリックします。

ステップ 15 [バウンスする（最終アクション）（Bounce (Final Action)）] を選択して、[OK] をクリックします。

コンテンツ フィルタに指定できる最終アクションは1つだけです。複数の最終アクションを追加しようとすると、GUI にエラーが表示されます。

このアクションを追加すると、この元従業員へのメッセージの送信者が、通知テンプレートとバウンス通知テンプレートの 2 つのメッセージを受け取る可能性があります。

ステップ 16 変更を送信し、保存します。

各受信者のグループごとのコンテンツ フィルタの適用

前述の例では、[受信メールポリシー（Incoming Mail Policy）] ページを使用して、3 つのコンテンツ フィルタを作成しました。[着信コンテンツフィルタ（Incoming Content Filters）] ページと [発信コンテンツフィルタ（Outgoing Content filters）] ページには、ポリシーに適用できるすべてのコンテンツフィルタの「プライマリリスト」が含まれています。

図 *9 : [受信コンテンツフィルタ（Incoming Content Filters）]*：作成された *3* つのフィルタ

この例では、[受信コンテンツフィルタ（Incoming Content Filters）] テーブルで使用される新しいコンテンツ フィルタを 3 つ適用します。

- デフォルト ポリシーには、3 つすべてのコンテンツ フィルタが適用されます。
- エンジニアリング グループには、no_mp3s フィルタは適用されません。
- 販売グループには、デフォルト着信メール ポリシーとしてコンテンツ フィルタが適用されます。

デフォルトでのすべての受信者のコンテンツ フィルタのイネーブル化

リンクをクリックして、個々のポリシーに対してコンテンツ フィルタをイネーブルにして選択します。

手順

ステップ 1 [受信メールポリシー（Incoming Mail Policies）] をクリックして、[受信メールポリシー（Incoming Mail Policy）] テーブルに戻ります。

ページがリフレッシュされ、デフォルト ポリシーおよび送信者および受信者のグループのメール ポリシーの作成 （5 ページ）で追加した 2 つのポリシーが表示されます。コンテンツ フィルタリングは、デフォルトでは、すべてのポリシーでディセーブルにされているため注意してください。

ステップ 2 デフォルト ポリシー行のコンテンツ フィルタ セキュリティ サービス（[コンテンツフィルタ（Content Filters）] 列）のリンクをクリックします。

ステップ 3 コンテンツ フィルタ セキュリティ サービス ページで、[コンテンツフィルタリング：デフォルトポリシー（Content Filtering for Default Policy）] の値を [コンテンツフィルタを無効にする（Disable Content Filters）] から [コンテンツフィルタを有効にする（設定をカスタマイズ）（Enable Content Filters (Customize settings)）] に変更します。

プライマリリストで定義されているコンテンツフィルタ（[受信コンテンツフィルタ（Incoming Content Filters）] ページを使用してコンテンツ フィルタの概要で作成されたフィルタ）が、このページに表示されます。値を [コンテンツフィルタを有効にする（設定をカスタマイズ）（Enable Content Filters (Customize settings)）] に変更すると、各フィルタのチェックボックスがディセーブル（グレー表示）からイネーブルに変わります。

ステップ 4 各コンテンツ フィルタの [有効（Enable）] チェックボックスをオンにします。

ステップ 5 [送信（Submit）] をクリックします。

[受信メール ポリシー（Incoming Mail Policies）] ページのテーブルは、デフォルト ポリシーで有効化されているフィルタの名前を示します。

エンジニアリングの受信者への MP3 添付ファイルの許可

「エンジニアリング」ポリシーの「no_mp3s」コンテンツ フィルタをディセーブルにするには、次の手順を実行します。

手順

ステップ 1 エンジニアリング チーム ポリシー行の [コンテンツフィルタセキュリティサービス（Content Filters security service）]（[コンテンツフィルタ（Content Filters）] 列）のリンクをクリックします。

ステップ 2 コンテンツ フィルタ セキュリティ サービス ページで、[ポリシーのコンテンツフィルタリング: エンジニアリング（Content Filtering for Policy: Engineering）] の値を [コンテンツフィルタを有効にする（デフォルトのメールポリシー設定を継承）（Enable Content Filtering (Inherit default policy settings)）] から [コンテンツフィルタを有効にする（設定をカスタマイズ）（Enable Content Filters (Customize settings)）] に変更します。

このポリシーはデフォルト値を使用していたため、値を [デフォルト設定を使用（Use Default Settings）] から [はい（Yes）] に変更すると、各フィルタのチェックボックスがディセーブル（グレー表示）からイネーブルに変わります。

ステップ 3 「no_mp3s」フィルタのチェックボックスの選択を解除します。

ステップ 4 [送信（Submit）] をクリックします。

[受信メールポリシー（Incoming Mail Policies）] ページのテーブルは、エンジニアリング ポリシーでイネーブルにされているフィルタの名前を示します。

ステップ 5 変更を保存します。

次のタスク

この時点では、エンジニアリング ポリシーのユーザ リストと一致する着信メッセージで MP3 添付ファイルは削除されません。ただし、他のすべての着信メッセージでは、MP3 添付ファイルが削除されます。

GUI でのコンテンツ フィルタの設定に関する注意事項

- コンテンツ フィルタを作成するときに条件を指定する必要はありません。アクションが定義されていない場合、定義されるアクションは常にルールに適用されます（アクションを指定しないことは、true() メッセージ フィルタ ルールを使用すること同じで、コンテンツ フィルタがポリシーに適用される場合、すべてのメッセージがマッチングされます）。
- カスタム ユーザー ロールをコンテンツ フィルタに割り当てていない場合、パブリックのコンテンツ フィルタになり、メール ポリシーの任意の委任管理者が使用できます。委任管理者とコンテンツ フィルタの詳細については、管理タスクの分散を参照してください。
- 管理者とオペレータは、コンテンツフィルタがカスタムユーザロールに割り当てられていない場合でも、アプライアンスのすべてのコンテンツフィルタを表示および編集できます。
- フィルタ ルールおよびアクションのテキストを入力する場合、正規表現照合において、次のメタ文字に特殊な意味があります。^ $ * + ? { [ ] \ | ( )

  正規表現を使用しない場合、「\」（バックスラッシュ）を使用して、これらの任意の文字をエスケープする必要があります。たとえば、「*Warning*」と入力します。

- コンテンツ フィルタに複数の条件を定義する場合、コンテンツ フィルタが一致したと見なされるために、定義されるアクションのすべて（論理 AND）、または定義されたいずれかのアクション（論理 OR）の適用が必要かどうかを定義できます。

メール ポリシーとコンテンツ フィルタの例

- 「benign」コンテンツ フィルタを作成して、メッセージ分裂およびコンテンツ フィルタをテストできます。たとえば、唯一のアクションが「配信」であるコンテンツ フィルタを作成できます。このコンテンツ フィルタは、メール処理に影響を与えませんが、このフィルタを使用して、メール ポリシー処理が、システムの他の要素（たとえば、メール ログ）に影響を与えているかテストできます。
- 逆に、着信コンテンツまたは発信コンテンツフィルタの「プライマリリスト」の概念を使用して、アプライアンスにより処理されるすべてのメールのメッセージ処理に即時に影響を与える、非常に優れた、広範囲に及ぶコンテンツフィルタを作成できます。このコンテンツ フィルタは次のように作成できます。
  - [受信コンテンツフィルタ（Incoming Content Filters）] または [送信コンテンツフィルタ（Outgoing Content filters）] ページを使用して、順序が 1 の新しいコンテンツ フィルタを作成します。
  - [受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（Outgoing Mail Policies）] ページを使用して、デフォルト ポリシーの新しいコンテンツ フィルタをイネーブルにします。
  - 残りすべてのポリシーでこのコンテンツ フィルタをイネーブルにします。
- コンテンツ フィルタで使用できる [Bcc:] および [隔離（Quarantine）] アクションは、作成する隔離エリアの保持設定に役に立ちます（詳細については、ポリシー、ウイルス、およびアウトブレイク隔離を参照してください）。メッセージがすぐにはシステムからリリースされないようにするため（つまり、隔離エリアの割り当てディスク領域がすぐにいっぱいにならないようにするため）、ポリシー隔離とのメールフローをシミュレートするフィルタを作成できます。
- scanconfig コマンドと同じ設定が使用されるため、「Entire Message」条件は、メッセージのヘッダーをスキャンしません。「Entire Message」を選択すると、メッセージ本文および添付ファイルだけがスキャンされます。特定のヘッダー情報を検索するには、「Subject」または「Header」条件を使用します。
- LDAP クエリによるユーザの設定は、アプライアンスで LDAP サーバが設定されている場合（つまり、ldapconfig コマンドを使用して特定の文字列を含む特定の LDAP サーバをクエリするようにアプライアンスが設定されている場合）だけ GUI に表示されます。
- リソースが事前に定義されていないため、コンテンツ フィルタ ルール ビルダのいくつかのセクションは、GUI に表示されません。たとえば、通知テンプレートおよびメッセージ免責事項は、[テキストリソース（Text Resources）] ページまたは CLI の textconfig コマンドを使用して事前に設定されていない場合、オプションとして表示されません。
- コンテンツフィルタ機能は、次の文字エンコーディングのテキストを認識し、これらを追加およびスキャンできます。
  - Unicode（UTF-8）
  - Unicode（UTF-16）
  - Western European/Latin-1（ISO 8859-1）
  - Western European/Latin-1（Windows CP1252）
  - 中国語（繁体字）（Big 5）
  - 中国語（簡体字）（GB 2312）

メール ポリシーとコンテンツ フィルタの例

- 中国語（簡体字）（HZ GB 2312）
- 韓国語（ISO 2022-KR）
- 韓国語（KS-C-5601/EUC-KR）
- 日本語（Shift-JIS（X0123））
- 日本語（ISO-2022-JP）
- 日本語（EUC）

複数の文字セットを1つのコンテンツ フィルタ内で組み合わせてマッチングできます。複数の文字エンコーディングでのテキストの表示および入力については、Webブラウザのマニュアルを参照してください。ほとんどのブラウザでは、複数の文字セットを同時にレンダリングできます。

図 *10*：コンテンツ フィルタでの複数の文字セット

- 着信または発信コンテンツ フィルタの要約ページで、[説明（Description）]、[ルール（Rules）] および [ポリシー（Policies）] のリンクを使用して、コンテンツ フィルタに提供されているビューを変更します。
  - [説明（Description）] ビューには、各コンテンツ フィルタの説明フィールドに入力したテキストが表示されます（これはデフォルト ビューです）。
  - [ルール（Rules）] ビューには、ルール ビルダ ページにより構築されたルールおよび正規表現が表示されます。
  - [ポリシー（Policies）] ビューには、イネーブルにされている各コンテンツ フィルタのポリシーが表示されます。

メール ポリシーとコンテンツ フィルタの例

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。