コンテンツ フィルタ

この章は、次の項で構成されています。

コンテンツ フィルタの概要

コンテンツ フィルタを使用して、アンチウイルス スキャンやDLP などのコンテンツ セキュリティ機能によって処理される標準ルーチン以上に、メッセージの処理をカスタマイズします。たとえばコンテンツ フィルタは、後で調査するためにコンテンツを隔離する必要がある場合や、企業のポリシーで特定メッセージを配信する前に暗号化する必要がある場合に使用できます。

コンテンツ フィルタの仕組み

コンテンツ フィルタは、電子メール パイプラインで後ほど適用される点、つまり、メッセージ フィルタリングの後で、1 つのメッセージが、各メール ポリシーに対応する個々の複数のメッセージに「分裂」された後で（詳細はメッセージ分裂を参照）、およびメッセージがアンチスパムおよびアンチウイルス スキャンされた後で適用される点を除いては、メッセージフィルタとほぼ同じです。

コンテンツ フィルタは、着信または発信メッセージをスキャンします。両方のメッセージをスキャンするフィルタを定義することはできません。電子メールゲートウェイには、各メッセージタイプのコンテンツフィルタに個別の「プライマリリスト」が用意されています。また、プライマリリストは、アプライアンスがコンテンツフィルタを実行する順序も決定します。ただし個々のメールポリシーは、メッセージがポリシーに一致するときに、実行される特定のフィルタを決定します。

コンテンツ フィルタは、ユーザー（送信者または受信者）単位でメッセージをスキャンします。

コンテンツ フィルタには次のコンポーネントがあります。

- どのような場合に電子メールゲートウェイがコンテンツフィルタを使用してメッセージをスキャンするかを決定する条件（任意）
- 電子メールゲートウェイがメッセージに実行するアクション（必須）
- メッセージを変更した場合に、電子メールゲートウェイがメッセージに追加できるアクション変数（任意）

関連項目

- コンテンツ フィルタを使用したメッセージ コンテンツのスキャン方法 （2 ページ）
- コンテンツ フィルタの条件 （3 ページ）
- コンテンツ フィルタのアクション （14 ページ）
- アクション変数 （24 ページ）

コンテンツ フィルタを使用したメッセージ コンテンツのスキャン方法

手順

	コマンドまたはアクション	目的
ステップ 1	（任意）コンテンツ フィルタがサポートする機能を定義します。	コンテンツ フィルタで使用する次の項目を作成します。 • 暗号化プロファイル • 免責事項テンプレート • 通知テンプレート • Policy 隔離 • URL 許可リスト
ステップ 2	着信または発信コンテンツ フィルタを定義します。	コンテンツ フィルタは以下で構成されることもあります。 • コンテンツ フィルタの条件 （3 ページ） （任意） • コンテンツ フィルタのアクション （14 ページ） • アクション変数 （24 ページ） （任意） コンテンツ フィルタの作成 （27 ページ）

	コマンドまたはアクション	目的
ステップ 3	コンテンツ セキュリティ ルールを設定するユーザ グループを定義します。	着信または発信メール ポリシーを作成します。
ステップ 4	フィルタを使用する着信または発信メッセージのユーザのグループにコンテンツ フィルタを割り当てます。	メール ポリシーを参照してください

コンテンツ フィルタの条件

条件は、電子メールゲートウェイが関連するメールポリシーに一致するメッセージにフィルタを使用するかどうかを決定する「トリガー」です。コンテンツ フィルタの条件の指定はオプションです。条件のないコンテンツ フィルタは関連するメール ポリシーに一致するすべてのメッセージに適用されます。

コンテンツ フィルタの条件では、メッセージ本文または添付ファイルで特定のパターンを検索するフィルタ ルールを追加する場合、パターンが検出される回数の最小しきい値を指定できます。AsyncOS はメッセージをスキャンすると、メッセージおよび添付ファイルに見つかった一致の数の「スコア」を集計します。最小しきい値に満たない場合、正規表現は true と評価されません。このしきい値は、テキスト、スマート ID、またはコンテンツ ディクショナリの用語に対して指定できます。

各フィルタには、複数の条件を定義できます。複数の条件が定義されている場合、条件を論理 OR（「次の任意の条件...」）または論理 AND（「次のすべての条件」）のいずれで結合するかを選択できます。

表 *1*：コンテンツ フィルタの条件

条件	説明
（条件なし）	コンテンツ フィルタでの条件の指定はオプションです。条件が指定されていない場合、true ルールが適用されます。true ルールはすべてのメッセージに一致し、必ずアクションが実行されます。

条件	説明
メッセージ本文または添付ファイル	[テキストを含む（Contains text）]：メッセージ本文に、特定のパターンと一致するテキストまたは添付ファイルが含まれているかどうかを判別します。 [スマート識別子を含む（Contains smart identifier）]：メッセージ本文または添付ファイルのコンテンツが、スマート ID と一致するかどうかを判別します。 • クレジット カード番号 • 米国社会保障番号 • Committee on Uniform Security Identification Procedures（CUSIP）番号 • American Banking Association（ABA; 米国銀行協会）ルーティング番号 [スマート識別子を含む（Contains smart identifier）]：メッセージ本文または添付ファイルのコンテンツが、プレフィックス（「credit」、「ssn」、「cusip」、または「aba」）を含むスマート識別子と一致するかどうかを判別します。 [コンテンツ辞書の単語を含む（Contains term in content dictionary）]：メッセージ本文に、<*dictionary name*> という名前のコンテンツ辞書のいずれかの正規表現または用語が含まれているかどうかを判別します。 このオプションをイネーブルにするには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリを参照してください。 （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ 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。 [要求された一致数（Number of matches required）]：true と評価するためにルールで必要な一致数を指定します。このしきい値は、テキスト、スマート ID、またはコンテンツ ディクショナリの用語に対して指定できます。 これには、配信ステータス部および関連付けられている添付ファイルが含まれます。

条件	説明
メッセージ本文	[テキストを含む（Contains text）]：メッセージ本文に、特定のパターンと一致するテキストが含まれているかどうかを判別します。 [スマート識別子を含む（Contains smart identifier）]：メッセージ本文のコンテンツが、スマート ID と一致するかどうかを判別します。スマート ID は、次のパターンを検出できます。 • クレジット カード番号 • 米国社会保障番号 • Committee on Uniform Security Identification Procedures（CUSIP）番号 • American Banking Association（ABA; 米国銀行協会）ルーティング番号 [スマート識別子を含む（Contains smart identifier）]：メッセージ本文のコンテンツが、プレフィックス（「credit」、「ssn」、「cusip」、または「aba」）を含むスマート識別子と一致するかどうかを判別します。 [コンテンツ辞書の単語を含む（Contains term in content dictionary）]：メッセージ本文に、<*dictionary name*> という名前のコンテンツ辞書のいずれかの正規表現または用語が含まれているかどうかを判別します。 このオプションをイネーブルにするには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリを参照してください。 （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ 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。 [要求された一致数（Number of matches required）]：true と評価するためにルールで必要な一致数を指定します。このしきい値は、テキストまたはスマート ID に対して指定できます。 このルールは、メッセージの本文だけに適用されます。添付ファイルまたはヘッダーは含まれません。
URL カテゴリ（URL Category）	URL レピュテーションまたは URL カテゴリによるフィルタリング：条件およびルールおよびURL カテゴリについてを参照してください。
メッセージ サイズ	本文サイズが、指定範囲内にあるかどうかを判別します。本文サイズとはメッセージのサイズのことで、ヘッダーと添付ファイルも含みます。本文サイズ ルールは、本文サイズが指定数と比較されるメッセージを選択します。

条件	説明
マクロ検出	受信または送信メッセージにマクロが有効な添付ファイルが含まれているか。 マクロ検出の条件を使用すると、選択したファイル タイプのメッセージのマクロが有効な添付ファイルを検出できます。
添付ファイルの内容	**[テキストを含む（Contains text）]**：指定したパターンと一致するテキストまたは別の添付ファイルが、メッセージの添付ファイルに含まれているか。このルールは body-contains() ルールと似ていますが、このルールでは、メッセージの全体の「本文」をスキャンしないようにします。つまり、ユーザが添付ファイルとして表示する場合だけスキャンします。 **[スマート識別子を含む（Contains a smart identifier）]**：メッセージ添付ファイルの内容が、指定されたスマート ID と一致するかどうかを判別します。 [スマート識別子を含む（Contains smart identifier）]：メッセージの添付ファイルのコンテンツが、プレフィックス（「credit」、「ssn」、「cusip」、または「aba」）を含むスマート識別子と一致するかどうかを判別します。 **[コンテンツ辞書の単語を含む（Contains terms in content dictionary）]**：添付ファイルに、<*dictionary name*> という名前のコンテンツ辞書のいずれかの正規表現または用語が含まれているかどうかを判別します。 ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリを参照してください。 （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ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。 [要求された一致数（Number of matches required）]：true と評価するためにルールで必要な一致数を指定します。このしきい値は、テキスト、スマート ID またはコンテンツ ディクショナリの一致回数に対して指定できます。

条件	説明
添付ファイルのファイル情報	

条件	説明
	[ファイル名（Filename）]：メッセージに、ファイル名が特定のパターンと一致する添付ファイルがあるかどうかを判別します。 **[コンテンツ辞書の単語を含むファイル名（Filename contains term in content dictionary）]**：メッセージに、<ディクショナリ名> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれるファイル名の添付ファイルがあるかどうかを判別します。 このオプションをイネーブルにするには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリを参照してください。 （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ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。 [ファイルタイプ（File type）]：メッセージに、フィンガープリントに基づいて特定のパターンと一致するファイル タイプの添付ファイルがあるかどうかを判別します（UNIX file コマンドと似ています）。 [MIMEタイプ（MIME type）]：メッセージに、特定の MIME タイプの添付ファイルがあるかどうかを判別します。このルールは attachment-type ルールに似ていますが、MIME 添付ファイルで指定された MIME タイプのみが評価される点が異なります。（電子メールゲートウェイは、ファイルタイプが明示的に指定されていない場合、拡張子からファイルのタイプを「予測」することはありません。） [ファイルハッシュリスト（File Hash List）]：メッセージに、特定のファイルの SHA-256 値と一致する添付ファイルがあるかどうかを判別します。ドロップダウンリストから必要なファイルハッシュリストを選択します。 （注） SHA-256 ファイルハッシュタイプを含むファイルハッシュリストのみ選択できます。 **[イメージ分析（Image Analysis）]**：メッセージに、指定されているイメージ判定と一致するイメージ添付ファイルがあるかどうかを判別します。有効なイメージ分析判定には、[疑わしい（Suspect）]、[不適切（Inappropriate）]、[不適切もしくは疑わしい（Suspect or Inappropriate）]、[スキャン不可（Unscannable）] または [正常（Clean）] があります。 [外部脅威フィード（External Threat Feeds）]：ファイルは選択した外部脅威フィードソースからの脅威情報と 一致していますか? [ファイルハッシュ例外リストの選択（Select a File Hash Exception List）]：（オプション） 電子メールゲートウェイで脅威を検出しない許可リスト登録済みファイルハッシュのリストを選択します。

条件	説明
	詳細については、外部脅威フィードを使用する電子メールゲートウェイの設定を参照してください。 **添付ファイルが破損しています（Attachment is Corrupt）**：破損した添付ファイルがメッセージに含まれているかどうか。 （注） 破損した添付ファイルとは、スキャンエンジンがスキャンできないため破損として識別する添付ファイルのことです。
添付ファイル保護	**[パスワードで保護されたまたは暗号化された添付ファイルが添付されている（Contains an attachment that is password-protected or encrypted）]**： （この条件は、たとえば、スキャンできない可能性がある添付ファイルを識別する場合に使用します）。 **[パスワードで保護されたまたは暗号化された添付ファイルが添付されていない（Contains an attachment that is NOT password-protected or encrypted）]**：
件名ヘッダー（Subject Header）	[件名ヘッダー（Subject Header）]：件名ヘッダーに、特定のパターンが含まれているかどうかを判別します。 [コンテンツ辞書の単語を含む（Contains terms in content dictionary）]：件名ヘッダーに、<ディクショナリ名>という名前のコンテンツディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。 ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリを参照してください。 （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ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。

条件	説明
その他のヘッダー	[ヘッダー名（Header name）]：メッセージに、特定のヘッダーが含まれているかどうかを判別します。 [ヘッダーの値（Header value）]：ヘッダーの値が、特定のパターンと一致するかどうかを判別します。 **[ヘッダーの値がコンテント辞書内の単語を含みます（Header value contains terms in the content dictionary）]**：指定されたヘッダーに、<ディクショナリ名> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。 ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリを参照してください （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ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。 このオプションを使用する方法を説明する例については、カスタム ヘッダーを使用して、陽性と疑わしいスパム内の URL を Cisco Web セキュリティ プロキシにリダイレクトする：設定例を参照してください。
エンベロープ送信者（Envelope Sender）	**[エンベロープ送信者（Envelope Sender）]**：エンベロープ送信者（Envelope From, <MAIL FROM>）が指定したパターンと一致しているか。 [LDAPグループに一致（Matches LDAP group）]：エンベロープ送信者（つまり、Envelope From、<MAIL FROM>）が、特定の LDAP グループに含まれるかどうかを判別します。 **[コンテンツ辞書の単語を含む（Contains term in content dictionary）]**：エンベロープ送信者に、<ディクショナリ名> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。 ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリを参照してください。 （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ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。

条件	説明
エンベロープ受信者	[エンベロープ受信者（Envelope Recipient）]：エンベロープ受信者（Envelope To, <RCPT TO>）が指定したパターンと一致しているか。 [LDAPグループに一致（Matches LDAP group）]：エンベロープ受信者（Envelope To, <RCPT TO>）が、指定した LDAP グループ内に存在するか。 **[コンテンツ辞書の単語を含む（Contains term in content dictionary）]**：エンベロープ受信者に、<ディクショナリ名>という名前のコンテンツディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。 ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリを参照してください。 （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ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。 [エンベロープ受信者（Envelope Recipient）]ルールは、メッセージ単位です。メッセージに複数の受信者がある場合、グループの受信者が 1 人でも検出されれば、指定されたアクションがメッセージのすべての受信者に適用されます。 エンベロープ送信者（Envelope From <MAIL FROM>）が、指定した LDAP グループ内に存在するか。
受信リスナー（Receiving Listener）	メッセージは、指定されたリスナー経由で届いたか。リスナー名は、システムで現在設定されているリスナーの名前である必要があります。
リモートIP（Remote IP）	リモートホストから送信されたメッセージは、指定したIPアドレスまたはIPブロックに一致しているか。[リモートIP（Remote IP）]ルールは、メッセージを送信したホストのIPアドレスが特定のパターンと一致するかどうかをテストします。これは、インターネット プロトコル バージョン 4（IPv4）またはバージョン 6（IPv6）アドレスを指定できます。IP アドレスパターンは、「送信者グループの構文」で説明されているように、許可されたホスト表記を使用して指定します。ただし、SBO、IPR、dnslist 表記および特殊キーワード ALL を除きます
レピュテーション スコア	送信者のIPレピュテーションスコアはいくつか。レピュテーション スコア ルールにより、IP レピュテーションスコアが別の値と比較してチェックされます。

条件	説明
DKIM 認証	DKIM 認証に合格したか、部分的に検証されたか、一時的に検証不可能として返されたか、失敗したか、DKIM 結果が返されていないかどうかを判別します。
偽装メールの検出	メッセージの送信元アドレスが偽装されているか。メッセージの From: ヘッダーがコンテンツ辞書のユーザに類似している場合にチェックするルールです。 コンテンツ ディクショナリを選択し、偽装の可能性ありとみなされるメッセージに、しきい値（1 ～ 100）を入力します。 偽装電子メール検出の条件は、From: ヘッダーとコンテンツ ディクショナリのユーザを比較します。このプロセス中に、類似により、 電子メールゲートウェイはディクショナリ内の各ユーザに類似性スコアを割り当てます。次に例を示します。 • From: ヘッダーが <j0hn.sim0ns@example.com> で、コンテンツディクショナリにユーザ「John Simons」が含まれている場合、 電子メールゲートウェイによってこのユーザに 82 の類似性スコアが割り当てられます。 • From: ヘッダーが <john.simons@diff-example.com> で、コンテンツディクショナリにユーザ「John Simons」が含まれている場合は、このユーザに 100 の類似性スコアが割り当てられます。 類似性スコアが高くなればなるほど、メッセージが偽装されている確立が高くなります。類似性スコアが指定したしきい値以上の場合は、フィルタ アクションがトリガーされます。 特定の送信者からのメッセージの偽装メールの検出フィルタをスキップする場合、[例外リスト（Exception List）] ドロップダウン リストからアドレス リストを選択します。 （注） 完全な電子メール アドレスを使用して作成したアドレス リストのみを選択できます。詳細については、着信接続ルールへの送信者アドレス リストの使用を参照してください。 詳細については、偽装メールの検出を参照してください。
SPF 検証	SPF 検証ステータスを判別します。このフィルタ ルールでは、さまざまな SPF 検証結果をクエリーできます。SPF 検証の詳細については、「電子メール認証」の章を参照してください。 （注） SPF ID を含まずに SPF 検証コンテンツ フィルタ条件を設定した場合、また異なる判定を含む異なる SPF ID がメッセージに含まれている場合は、メッセージ内のいずれかの判定と一致した条件がトリガーされます。

条件	説明
S/MIME ゲートウェイ メッセージ（S/MIME Gateway Message）	メッセージは S/MIME 署名されているか、暗号化されているか、または署名および暗号化されているか。詳細については、S/MIME セキュリティ サービスを参照してください。
S/MIME ゲートウェイ 検証済	S/MIME メッセージは正常に検証されているか、復号されているか、または復号および検証されているか。詳細については、S/MIMEセキュリティ サービスを参照してください。
メッセージ言語	メッセージ（件名と本文）は選択したいずれかの言語であるか。この条件では、添付ファイルおよびヘッダーの言語は確認しません。 **言語の検出の動作の仕組み** 電子メールゲートウェイは、メッセージの言語を検出するのに組み込みの言語検出エンジンを使用します。電子メールゲートウェイは、件名とメッセージ本文を抽出し、言語検出エンジンに渡します。 言語検出エンジンは、抽出されたテキスト内の各言語の確率を決定し、それを電子メールゲートウェイに渡します。電子メールゲートウェイは、最も高い確率をもつ言語をメッセージの言語とみなします。 電子メールゲートウェイは、次のシナリオのいずれかで、メッセージの言語を「判別不能」とみなします。 • 検出された言語が 電子メールゲートウェイでサポートされていない場合 • 電子メールゲートウェイがメッセージの言語を検出できない場合 • 言語検出エンジンに送られた抽出されたテキストの合計サイズが 50 バイト未満の場合。
重複境界検証	そのメッセージに、重複する MIME 境界が含まれるか。 重複する MIME 境界が含まれるメッセージにアクションを実行する場合は、この条件を使用します。 （注） 添付ファイルベースの条件（たとえば、添付ファイルの内容）や操作（たとえば、コンテンツによる添付ファイルの除去）は、（重複する MIME 境界を含む）不正なメッセージでは動作しません。
位置情報	メッセージが選択した国で作成されたものかどうかを判別します。 位置情報条件を使用すると、選択した特定の国からの着信メッセージを処理できます。 （注） 位置情報コンテンツフィルタを使用する前に、電子メールゲートウェイでスパム対策エンジンを有効にします。

条件	説明
ドメインのレピュテーション	送信者ドメインは、指定された基準と一致していますか? • 送信者ドメインのレピュテーション • 外部脅威フィード 詳細については、外部脅威フィードを使用する電子メールゲートウェイの設定または送信者ドメイン レピュテーション フィルタリングを参照してください。

コンテンツ フィルタのアクション

アクションは、電子メールゲートウェイがコンテンツフィルタの条件に一致するメッセージに行うことです。メッセージの変更、隔離またはドロップなどさまざまなタイプのアクションが用意されています。メッセージで配信またはドロップといった「最終アクション」が実行されることで、E メール セキュリティ アプライアンスで強制的にアクションが即時実行され、アウトブレイク フィルタまたは DLP スキャンなどのその後のすべての処理が実施されません。

各コンテンツ フィルタには、少なくとも 1 つのアクションを定義する必要があります。

アクションは、順序に従いメッセージで実行されるため、コンテンツ フィルタの複数のアクションを定義する場合、アクションの順序を考慮します。

Attachment Content 条件、Message Body または Attachment 条件、Message 本文条件、または Attachment 内容条件と一致するメッセージに対して隔離アクションを設定した場合、隔離されたメッセージ内の一致した内容を表示できます。メッセージ本文を表示すると、一致した内容が黄色で強調表示されます。また、$MatchedContent アクション変数を使用して、一致した内容をメッセージの件名に含めることができます。詳細については、「テキスト リソース」の章を参照してください。

フィルタごとに定義できる最終アクションは1つだけです。最終アクションは、リストの最後のアクションです。バウンス、配信、およびドロップは、最終アクションです。コンテンツフィルタのアクションを入力する場合、GUIおよびCLIにより、最終アクションが強制的に最後に配置されます。

アクション変数 （24 ページ）も参照してください。

表 *2:* コンテンツ フィルタのアクション

アクション	説明
検疫（Quarantine）	[隔離（Quarantine）]。いずれかの Policy 隔離エリアに保持されるメッセージにフラグを付けます。 [重複するメッセージ（Duplicate message）]：メッセージのコピーを指定された隔離エリアに送信して、オリジナル メッセージの処理を続行します。任意の追加アクションが、オリジナル メッセージに適用されます。
配信時の暗号化	メッセージは、次の処理段階に進みます。すべての処理が完了すると、メッセージが暗号化され、配信されます。 [暗号化ルール（Encryption rule）]：メッセージを常に暗号化するか、TLS接続を介した送信試行が最初に失敗した場合だけ暗号化します。詳細については、TLS接続を暗号化の代わりに使用を参照してください。 **[暗号化プロファイル（Encryption Profile）]**：処理が完了したら、指定された暗号化プロファイルを使用してメッセージを暗号化し、メッセージを配信します。このアクションは、Cisco 暗号化アプライアンスまたはホステッド キー サービスと併用します。 **[件名（Subject）]**：暗号化されたメッセージの件名です。デフォルト値は **`$Subject`** です。
内容によって添付ファイルを除去	**[次を含む添付ファイル（Attachment contains）]**：正規表現を含むメッセージのすべての添付ファイルをドロップします。アーカイブ ファイル（zip、tar）は、中に含まれているファイルのいずれかが正規表現と一致する場合にドロップされます。 **[スマート識別子を含む（Contains smart identifier）]**：指定されたスマート ID を含むメッセージのすべての添付ファイルをドロップします。 **[コンテンツ辞書の単語を含む添付ファイル（Attachment contains terms in the content dictionary）]**：添付ファイルに、*<dictionary name>* という名前のコンテンツ辞書のいずれかの正規表現または用語が含まれているかどうかを判別します。 [要求された一致数（Number of matches required）]：true と評価するためにルールで必要な一致数を指定します。このしきい値は、テキスト、スマート ID またはコンテンツ ディクショナリの一致回数に対して指定できます。 **[メッセージ差し替え（Replacement message）]**：オプション コメントは、ドロップされた添付ファイルの置換に使用されるテキストを変更します。添付ファイルのフッターは、単純にメッセージに追加されるだけです。

アクション	説明
ファイル情報によって添付ファイルを除去	

アクション	説明
	[ファイル名（File name）]：指定された正規表現とファイル名が一致するメッセージのすべての添付ファイルをドロップします。アーカイブ形式の添付ファイル（zip、tar）内に該当するファイルがある場合、この添付ファイルはドロップされます。 [ファイルサイズ（File size）]：メッセージの添付ファイルのうち、ロー エンコード形式で指定したサイズ（バイト単位）以上のサイズであるファイルをすべてドロップします。アーカイブ ファイルまたは圧縮ファイルの場合、このアクションは、圧縮前のサイズを検証せず、実際の自体のサイズが計測されます。 [ファイルタイプ（File type）]：メッセージの添付ファイルのうち、指定したファイルの「フィンガープリント」と一致するファイルをすべてドロップします。アーカイブ形式の添付ファイル（zip、tar）内に該当するファイルがある場合、この添付ファイルはドロップされます。 [MIMEタイプ（MIME type）]：メッセージの添付ファイルのうち、特定の MIME タイプのファイルをすべてドロップします。 [ファイルハッシュリスト（File Hash List）]：選択したファイルハッシュリスト内のファイルの SHA-256 値と一致するメッセージにあるすべての添付ファイルをドロップします。ドロップダウンリストから必要なファイルハッシュリストを選択します。 （注） SHA-256 ファイルハッシュタイプを含むファイルハッシュリストのみ選択できます。 [イメージ分析判定（Image Analysis Verdict）]：指定されたイメージ判定と一致するイメージ添付ファイルをドロップします。有効なイメージ分析判定には、[疑わしい（Suspect）]、[不適切（Inappropriate）]、[不適切もしくは疑わしい（Suspect or Inappropriate）]、[スキャン不可（Unscannable）] または [正常（Clean）] があります。 **外部脅威フィード**。ETFエンジンによって悪意のあるファイルとして分類されたメッセージのすべてのメッセージ添付ファイルをドロップします。 **ファイル ハッシュ例外リストを選択します。**（任意）Cisco E メール セキュリティ ゲートウェイで脅威を検出しない許可リスト登録済みファイルハッシュのリストを選択します。 詳細については、外部脅威フィードを使用する電子メールゲートウェイの設定を参照してください。 **[メッセージ差し替え（Replacement message）]**：オプション コメントは、ドロップされた添付ファイルの置換に使用されるテキストを変更します。添付ファイルのフッターは、単純にメッセージに追

アクション	説明
	加されるだけです。
マクロが含まれる添付ファイルを削除	指定したファイル タイプのマクロが有効になった添付ファイルをすべてドロップします。 （注） アーカイブまたは埋め込みファイルにマクロが含まれている場合、親ファイルはメッセージからドロップされます。 [カスタム差し替えメッセージ（Custom Replacement Message）]（任意）：添付ファイルが削除されるとき、デフォルトでは、システム生成のメッセージがメッセージ本文の一番下に追加されます。 以下は、マクロが有効な添付ファイルがメッセージから削除されるときにシステムによって生成されるメッセージのサンプルです。 **A MIME attachment of type <application/vnd.ms-excel> was removed here by a drop-macro-enabled-attachments filter rule on the host <mail.example.com>.** [カスタム差し替えメッセージ（Custom Replacement Message）] フィールドにカスタム メッセージを入力すると、システム生成のメッセージは入力されたメッセージに差し替えられます。
URLレピュテーション（URL Reputation）	メッセージに含まれるURLの変更：フィルタでのURLレピュテーションまたはURLカテゴリのアクションの使用およびURLフィルタリングの許可リストの作成を参照してください。 レピュテーションを判断できないURLには、「スコアなし」を使用してアクションを指定します。 （注） S/MIMEを使用して暗号化されている場合またはS/MIME署名が含まれる場合、電子メールゲートウェイはメッセージを署名済みとみなします。
URLカテゴリ（URL Category）	メッセージに含まれるURLの変更：フィルタでのURLレピュテーションまたはURLカテゴリのアクションの使用およびURLカテゴリについてを参照してください。 （注） S/MIMEを使用して暗号化されている場合またはS/MIME署名が含まれる場合、電子メールゲートウェイはメッセージを署名済みとみなします。

アクション	説明
免責条項文の追加	[上に配置（Above）]：メッセージ上部に免責事項を追加します（ヘッダー）。 **[下に配置（Below）]**：メッセージ下部に免責事項を追加します（フッター）。 **注**：このコンテンツ フィルタ アクションを使用するには、免責事項テキストをすでに作成している必要があります。 詳細については、免責事項テンプレートを参照してください。
アウトブレイク フィルタによるスキャンのバイパス	メッセージに対してアウトブレイク フィルタによるスキャンをスキップします。
DKIM 署名のバイパス	メッセージに対して DKIM 署名をバイパスします。
コピー（Bcc:）を送信	[電子メールアドレス（Email addresses）]：指定受信者にメッセージを匿名でコピーします。 **[件名（Subject）]**：コピーされたメッセージの件名を追加します。 **[リターンパス（オプション）（Return path (optional)）]**：リターン パスを指定します。 **[代替メールホスト（オプション）（Alternate mail host (optional)）]**：代替メール ホストを指定します。
通知	**[通知（Notify）]**：指定された受信者にこのメッセージを報告します。オプションで送信者および受信者に通知できます。 **[件名（Subject）]**：コピーされたメッセージの件名を追加します。 **[リターンパス（オプション）（Return path (optional)）]**：リターン パスを指定します。 [テンプレート利用（Use template）]：作成したテンプレートからテンプレートを選択します。 [オリジナル メッセージを添付ファイルとして含めます（Include original message as an attachment）]：オリジナル メッセージを添付ファイルとして追加します。
受信者を変更	**電子メール アドレス**メッセージの受信者を指定電子メール アドレスに変更します。

アクション	説明
代替送信ホストにメッセージを送信	[メールホスト（Mail host）]：メッセージの宛先メール ホストを指定メール ホストに変更します。 （注） このアクションは、アンチスパム スキャン エンジンによりスパムとして分類されたメッセージが隔離されないようにします。このアクションは、隔離を無効にして、指定メール ホストに送信します。
IP インターフェイスから送信	**[次の IP インターフェイスから送信（Send from IP interface）]**：指定 IP インターフェイスから送信します。[IP インターフェイスから送信（Deliver from IP Interface）] アクションは、メッセージのソース ホストを指定ソースに変更します。ソース ホストは、メッセージが配信される IP インターフェイスで構成されます。
ヘッダーの除去	**[ヘッダー名（Header name）]**：指定ヘッダーを配信前にメッセージから削除します。
ヘッダーの追加/編集	**メッセージに新しいヘッダーを挿入または既存のヘッダーを変更します。** [ヘッダー名（Header name）]：新規または既存のヘッダーの名前。 **[新しいヘッダーの値を指定（Specify value of new header）]**：新しいヘッダーの値を配信前にメッセージに挿入します。 **[既存のヘッダーの値の前に付加（Prepend to the Value of Existing Header）]**：配信前に既存のヘッダーの前に値を追加します。 **[既存のヘッダーの値の後ろに付加（Append to the Value of Existing Heade）]**：配信前に既存のヘッダーの後ろに値を追加します。 [既存のヘッダーの値から検索して置換（Search & Replace from the Value of Existing Header）]：[検索対象（Search for）] フィールドに、既存のヘッダーで置き換える値を見つけるための検索語を入力します。ヘッダーに挿入する値を [次で置換（Replace with）] フィールドに入力します。値を検索するために正規表現を使用できます。ヘッダーから値を削除する場合は、[次で置換（Replace with）] フィールドを空白のままにしてください。
偽装メールの検出	偽装されたメッセージから From: ヘッダーを削除し、エンベロープ送信者で置き換えます。 偽装メールの検出を参照してください。

アクション	説明
メッセージ タグの追加	DLP ポリシー フィルタリングで使用するカスタム用語をメッセージに挿入します。DLP ポリシーを設定して、スキャン対象をメッセージタグがあるメッセージに限定することができます。メッセージタグは受信者側では表示されません。DLPポリシーでのメッセージ タグの使用については、データ損失防止のポリシーを参照してください。
ログ エントリの追加	カスタマイズされたテキストを INFO レベルで IronPort テキスト メール ログに挿入します。このテキストにはアクション変数を使用することができます。ログ エントリはメッセージ トラッキングにも表示されます。

アクション	説明
CEF ログエントリの追加	カスタマイズされたテキストを統合イベントログに挿入します。このテキストにはアクション変数を使用することができます。 （注） このコンテンツ フィルターアクションは、電子メールゲートウェイで「統合イベントログ」ログサブスクリプションを設定する場合にのみ使用できます。 [ラベル（Label）]：統合イベントログエントリのラベルを追加します。 （注） ログラベルは、64 文字を超えてはなりません。 [値（Value）]：統合イベントログエントリのメッセージを追加します。 （注） メッセージは、1024 文字を超えてはなりません。 （注） 電子メールゲートウェイでは、Syslog プッシュ方式で統合イベントログを使用する場合、CEF ログ行に 65535 文字の制限があります。外部の SIEM ソリューションには、CEF ログファイルに許可される文字数に制限が定義されている場合もあります。電子メールゲートウェイと SIEM ソリューションで許可されている文字数に基づいて、ログに記録されるカスタマイズしたテキストと統合イベントログサブスクリプションフィールドを適切に設定してください。 [選択したログフィールド（Selected Log Fields）] にある [カスタムログエントリ（Custom Log Entries）] を使用して [統合イベントログ（Consolidated Event Logs）] ログサブスクリプションを設定すると、CEF ログエントリが [統合イベントログ（Consolidated Event Logs）] に表示されます。 **例**：[ラベル（Label）] フィールドに「label1」、[値（Value）] フィールドに「value20」と入力すると、次のフィールドが統合イベントログに追加されます。 `ESACustomLogs={'label1': ['value20']}`
配信時の S/MIME 署名/暗号化	配信時にメッセージの S/MIME 署名または暗号化を実行します。メッセージは次の処理段階に進み、すべての処理が完了した時点で署名または暗号化されて、配信されます。 **S/MIME 送信プロファイル**：指定された S/MIME 送信プロファイルを使用して、S/MIME 署名または暗号化を実行します。S/MIME 送信プロファイルの管理を参照してください。

アクション	説明
暗号化して今すぐ配信（最終アクション）	メッセージを暗号化および配信し、その後の任意の処理をスキップします。 [暗号化ルール（Encryption rule）]：メッセージを常に暗号化するか、TLS接続を介した送信試行が最初に失敗した場合だけ暗号化します。詳細については、TLS接続を暗号化の代わりに使用を参照してください。 **[暗号化プロファイル（Encryption Profile）]**：指定された暗号化プロファイルを使用してメッセージを暗号化し、メッセージを配信します。このアクションは、Cisco 暗号化アプライアンスまたはホステッド キー サービスと併用します。 **[件名（Subject）]**：暗号化されたメッセージの件名です。デフォルト値は **`$Subject`** です。
S/MIME 署名/暗号化（最終アクション）	S/MIME 署名または暗号化を実行してメッセージを配信し、その後の処理はスキップします。 **S/MIME 送信プロファイル**：指定された S/MIME 送信プロファイルを使用して、S/MIME 署名または暗号化を実行します。S/MIME 送信プロファイルの管理を参照してください。
バウンスする（最終アクション）	メッセージを送信者に戻します。
残りのコンテンツ フィルタをスキップ（最終アクション）	メッセージを次の処理段階に配信し、その後の任意のコンテンツ フィルタをスキップします。設定に応じて、メッセージが受信者に配信されるか、隔離が実行されるか、アウトブレイク フィルタによるスキャンが開始されます。
ドロップする（最終アクション）	メッセージをドロップして廃棄します。

アクション	説明
Safe Print	「Safe Print」コンテンツ フィルタ アクションを使用して、メッセージの添付ファイルを Safe Print で出力します。 Safe Print コンテンツ フィルタ アクションは、次のいずれかの方法で使用できます。 • 一致する添付ファイルをSafe Printで出力（Safe print matching attachments）：このオプションを使用すると、設定されたコンテンツ フィルタ条件に一致するすべてのメッセージの添付ファイルを Safe Print で出力します。 • すべての添付ファイルをSafe Printで出力（Safe print all attachments）：このオプションを使用すると、設定されたコンテンツ フィルタ条件が true の場合にすべてのメッセージの添付ファイルを Safe Print で出力します。 [はい（Yes）] を選択して、スキャン不可とマークされているメッセージの添付ファイルを削除します。 （注） デフォルトでは、添付ファイルがスキャンできない場合、システム生成のメッセージが添付テキスト ファイルとして追加されます。[カスタム差し替えメッセージ（Custom Replacement Message）] フィールドにカスタム メッセージを入力します。 詳細については、メッセージの添付ファイルを Safe Print で出力する場合の電子メール ゲートウェイの設定方法を参照してください。

関連項目

- アクション変数 （24 ページ）

アクション変数

コンテンツ フィルタにより処理されるメッセージに追加されるヘッダーには、アクション実行時にオリジナル メッセージの情報に自動的に置換される変数を含めることができます。これらの特殊な変数はアクション変数と呼ばれます。電子メールゲートウェイでは次のアクション変数がサポートされています。

表 *3:* アクション変数

変数	構文	説明
すべてのヘッダー（All Headers）	`$AllHeaders`	メッセージ ヘッダーに置き換えられます。

変数	構文	説明
本文サイズ（Body Size）	`$BodySize`	メッセージのサイズ（バイト単位）に置き換えられます。
日付（Date）	`$Date`	現在の日付（MM/DD/YYYY 形式）に置き換えられます。
ドロップされたファイル名（Dropped File Name）	`$dropped_filename`	直近にドロップされたファイル名のみを返します。
ドロップされたファイル名（Dropped File Names）	`$dropped_filenames`	$filenames と同様に、ドロップされたファイルのリストを表示します。
ドロップされたファイルタイプ（Dropped File Types）	`$dropped_filetypes`	$filetypes と同様に、ドロップされたファイルタイプのリストを表示します。
エンベロープ送信者（Envelope Sender）	`$envelopefrom` or `$envelopesender`	メッセージのエンベロープ送信者（Envelope From、<MAIL FROM>）に置き換えられます。
エンベロープ受信者（Envelope Recipients）	`$EnvelopeRecipients`	メッセージのエンベロープ受信者すべて（Envelope To、<RCPT TO>）に置き換えられます。
ファイル名（File Names）	`$filenames`	メッセージの添付ファイルのファイル名のカンマ区切リストに置き換えられます。
ファイルサイズ（File Sizes）	`$filesizes`	メッセージの添付ファイル サイズのカンマ区切りリストに置き換えられます。
ファイルタイプ（File Types）	`$filetypes`	メッセージの添付ファイルのファイル タイプを示すカンマ区切りリストに置き換えられます。
フィルタ名（Filter Name）	`$FilterName`	処理されるフィルタの名前に置き換えられます。
GMT 日時（GMTimeStamp）	`$GMTimeStamp`	現在の時刻および日付（GMT）に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。
HATグループ名（HAT Group Name）	`$Group`	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。

変数	構文	説明
メールフローポリシー（Mail Flow Policy）	`$Policy`	メッセージのインジェクト時に、送信者に適用したHATポリシーの名前に置き換えられます。事前に定義されているポリシー名が使用されていない場合、文字列「>Unknown<」が挿入されます。
一致した内容（Matched Content）	`$MatchedContent`	コンテンツスキャンフィルタをトリガーした1つ以上の値に置き換えられます。一致した内容は、コンテンツディクショナリマッチ、スマートIDまたは正規表現との一致になります。
ヘッダー（Header）	`$Header['string']`	元のメッセージに一致するヘッダーが含まれる場合、引用符付きヘッダーの値に置き換えられます。二重引用符が使用される場合もあります。
ホストネーム	`$Hostname`	電子メールゲートウェイのホスト名に置き換えられます。
内部メッセージID（Internal Message ID）	`$MID`	メッセージを内部で識別するために使用するメッセージID（MID）に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください（「Message-Id」を取得するには$Headerを使用します）。
受信リスナー（Receiving Listener）	`$RecvListener`	メッセージを受信したリスナーのニックネームに置き換えられます。
受信インターフェイス（Receiving Interface）	`$RecvInt`	メッセージを受信したインターフェイスのニックネームに置き換えられます。
リモートIPアドレス（Remote IP Address）	`$RemoteIP`	メッセージを電子メールゲートウェイに送信したシステムのIPアドレスに置き換えられます。
リモートホストアドレス（Remote Host Address）	`$remotehost`	メッセージを電子メールゲートウェイに送信したシステムのホスト名に置き換えられます。
SenderBase レピュテーション スコア	`$Reputation`	送信者のSenderBaseレピュテーションスコアに置き換えられます。レピュテーションスコアがない場合は「None」に置き換えられます。
Subject	`$Subject`	メッセージの件名に置き換えられます。

変数	構文	説明
時刻	`$Time`	現在の時刻（ローカル時間帯）に置き換えられます。
Timestamp	`$Timestamp`	現在の時刻および日付（ローカル時間帯）に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。

コンテンツに基づくメッセージのフィルタリング方法

関連項目

- コンテンツ フィルタの作成 （27 ページ）
- 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 （29 ページ）
- 特定のユーザ グループに対するメッセージへのコンテンツ フィルタの適用 （29 ページ）
- GUI でのコンテンツ フィルタの設定に関する注意事項 （30 ページ）

コンテンツ フィルタの作成

はじめる前に

- コンテンツ フィルタに一致するメッセージを暗号化する場合は、暗号化プロファイルを作成します。
- 一致メッセージに免責事項を追加する場合は、免責事項の生成に使用する免責事項テンプレートを作成します。
- 一致するメッセージについてユーザに通知メッセージを送信する場合は、通知を生成するための通知テンプレートを作成します。
- メッセージを隔離する場合は、これらのメッセージに対する新しいPolicy隔離を作成するか、または既存のものを使用します。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] をクリックします。

または

[メールポリシー（Mail Policies）] > [送信メールポリシー（Outgoing Mail Policies）] をクリックします。

ステップ 2 [フィルタの追加（Add Filter）] をクリックします。

ステップ 3 フィルタの名前と説明を入力します。

ステップ 4 （相互参照）[編集可能なユーザ（役割）（Editable By (Roles)）] リンクをクリックして、ポリシーの管理者を選択し、[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 5 （任意）フィルタをトリガーするための条件を追加します。

a) [条件を追加（Add Condition）] をクリックします。
b) 条件のタイプを選択します。
c) 条件のルールを定義します。
d) [OK] をクリックします。
e) フィルタに追加する追加条件について、上記の手順を繰り返して行ってください。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。

（注） 条件を追加しない場合、電子メールゲートウェイはフィルタに関連するメールポリシーの 1 つと一致するあらゆるメッセージにコンテンツフィルタのアクションを実行します。

ステップ 6 フィルタの条件に一致するメッセージに対して実行する電子メールゲートウェイのアクションを追加します。

a) [アクションを追加（Add Action）] をクリックします。
b) アクション タイプを選択します。
c) アクションを定義します。
d) [OK] をクリックします。
e) 電子メールゲートウェイに実行する追加のアクションについて、上記の手順を繰り返して行ってください。
f) 複数のアクションに対して、電子メールゲートウェイがメッセージに適用する順序でアクションを配置します。フィルタごとに 1 個だけ「最終」アクションがあり、AsyncOS は自動的に最終アクションを順番の最後に移動します。

ステップ 7 変更を送信し、保存します。

次のタスク

- デフォルトの着信または発信メール ポリシーでコンテンツ フィルタをイネーブルにできます。
- 特定のユーザ グループのメールポリシーのコンテンツ フィルタをイネーブルにできます。

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

手順

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

または

[メールポリシー（Mail Policies）] > [送信メールポリシー（Outgoing Mail Policies）] をクリックします。

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（コンテンツ フィルタの概要 （1 ページ）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イネーブルになります。

ステップ 4 イネーブルにする個々のコンテンツ 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 変更を送信し、保存します。

特定のユーザ グループに対するメッセージへのコンテンツ フィルタの適用

はじめる前に

- ユーザー グループのメッセージに対してコンテンツ フィルタを使用する場合、着信または発信メールポリシーを作成します。詳細については、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）] > [受信メールポリシー（Incoming Mail Policies）] をクリックします。

または

[メールポリシー（Mail Policies）] > [送信メールポリシー（Outgoing Mail Policies）] をクリックします。

ステップ 2 コンテンツ フィルタに適用するメール ポリシーのコンテンツ 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、[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。

ステップ 4 ユーザが使用するコンテンツ フィルタのチェックボックスを選択します。

ステップ 5 変更を送信し、保存します。

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（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）。
- カスタム ユーザ 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、「Common Administrative Tasks」の章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る場合でも、電子メールゲートウェイ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。

- 「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、電子メール セキュリティ マネージャ 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、電子メールゲートウェイ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、電子メールゲートウェイで 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）
  - 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。

- 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。

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。