



## CHAPTER 6

# 電子メール セキュリティ マネージャ

電子メール セキュリティ マネージャは、IronPort アプライアンスのすべての電子メール セキュリティ サービスおよびアプリケーションを管理するための1つの包括的なダッシュボードです。本リリースよりも前のリリースでは、アンチスパムおよびアンチウイルス設定は、リスナー単位で行われていました。つまり、ポリシーは、メッセージの受信者または送信者に基づいてではなく、IP アドレスの受信リスナーに基づいて適用されていました。第5章「電子メールを受信するためのゲートウェイの設定」では、リスナーの作成および設定方法について説明します。

電子メール セキュリティ マネージャを使用すると、ウイルス感染フィルタ機能、アンチスパム、アンチウイルスおよび電子メール コンテンツ ポリシーを、個別のインバウンドおよびアウトバウンド ポリシーを介して、受信者または送信者単位で管理できます。

GUI の [Mail Policies] メニュー (CLI の `policyconfig` コマンド) を使用して、着信または発信メール ポリシーを作成および管理します。メール ポリシーは、次の機能の特定の設定にマッピングされるユーザの特定のセットとして定義されます (エンベロープ受信者、エンベロープ送信者、From: ヘッダーまたは Reply-To: ヘッダー)。

- アンチスパム スキャン
- アンチウイルス スキャン
- ウイルス感染フィルタ
- コンテンツ フィルタ

ユーザは、電子メール アドレス、電子メール ドメインまたは LDAP グループ クエリーにより定義できます。

この章は、次の内容で構成されています。

- 「ユーザベース ポリシーの概要」 (P.6-190)
- 「コンテンツ フィルタの概要」 (P.6-198)
- 「実際の例 (GUI)」 (P.6-219)

## ユーザベース ポリシーの概要

電子メール セキュリティ マネージャのユーザベース ポリシーを使用すると、組織内のすべてのユーザのさまざまな、また個別のセキュリティ ニーズを満たすポリシーを作成できます。

たとえば、この機能を使用すると、次の条件を適用するポリシーをすぐに作成できます。

- **IronPort Anti-Spam** スキャンを、販売部へのすべての電子メールではディセーブルにし、エンジニアリング部では、陽性と疑わしいスパム メッセージと問題のないマーケティング メッセージの件名にタグを付け、陽性と判定されたスパムをドロップする中程度のポリシーを適用してイネーブルにします。また、人事部では、陽性と疑わしいスパム メッセージと問題のないマーケティング メッセージを検疫して、陽性と判定されたスパムをドロップする、積極的なポリシーを適用してアンチスパム スキャンをイネーブルにします。
- システム管理者グループ以外のすべてのユーザで、危険な実行可能プログラムの添付ファイルをドロップします。
- エンジニアリング部宛てのメッセージのウイルスをスキャンおよび修復しますが、アドレス `jobs@example.com` に送信されるすべてのメッセージの感染添付ファイルをドロップします。
- **RSA Email DLP** を使用してすべての発信メッセージをスキャンし、機密情報として扱う必要のある情報が含まれているかどうか確認します。条件と一致するメッセージは、検疫され、法務部にブラインド カーボン コピーで送信されます。
- 着信メッセージに **MP3** 添付ファイルが含まれている場合、そのメッセージを検疫して、宛先となっている受信者に、メッセージを受信するにはネットワーク オペレーション センターに問い合わせる必要があることを示すメッセージを送信します。このようなメッセージは 10 日後に有効期限が切れません。

- エグゼクティブ スタッフからのすべての発信メールへの免責事項を企業の最新のタグ ラインに含め、広報部からのすべての発信メールに異なる「将来の見込みに関する」免責事項を含めます。
- すべての着信メッセージのウイルス感染フィルタ機能をイネーブルにして、ファイル拡張子が .dwg の添付ファイルを含むメッセージのスキャンをバイパスします。

**(注)**

コンテンツ フィルタから、コンテンツ ディクショナリ、免責事項および通知に関するテンプレートを参照するには、これらを事前に作成しておく必要があります。詳細については、「[テキスト リソース](#)」(P.14-429) を参照してください。

## 着信および 発信メッセージ

電子メール セキュリティ マネージャでは、2 つのポリシー テーブルが定義されます。1 つは、HAT ポリシーにより「Accept」動作として規定される送信ホストからのメッセージ用のテーブルで、もう 1 つのテーブルは、HAT「Relay」動作と見なされる送信ホスト用のテーブルです。前者のテーブルは、**着信**ポリシー テーブルで、後者は、**発信**ポリシー テーブルです。

- **着信**メッセージは、任意のリスナーの ACCEPT HAT ポリシーに一致する接続から受信されるメッセージです。
- **発信**メッセージは、任意のリスナーの RELAY HAT ポリシーに一致する接続からのメッセージです。この接続には、SMTP AUTH で認証された任意の接続が含まれます。

**(注)**

特定のインストールでは、IronPort アプライアンスを経由する「内部」メールは、すべての受信者が内部アドレスにアドレス指定されている場合でも、**発信**と見なされます。たとえば、IronPort C150/160 カスタマーの場合はデフォルトで、System Setup Wizard がインバウンド電子メールの受信およびアウトバウンド電子メールのリレー用として、1 リスナーに物理イーサネット ポートを 1 つだけ設定します。

多くの設定では、いずれもシングル リスナーにより使用される場合でも、着信テーブルはパブリック、発信テーブルはプライベートと見なされます。特定のメッセージで使用されるポリシー テーブルは、メッセージの方向、つまり、送信者アドレスか受信者アドレスかどうか、またはインターネットへの発信かイントラネットへの着信かどうかによって依存しません。

これらのテーブルを管理するには、GUI の [Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページ、あるいは CLI の `policyconfig` コマンドを使用します。

## ポリシー マッチング

着信メッセージがシステムのリスナーにより受信されると、システムで設定されているリスナーの数に関係なく、各メッセージ受信者は、いずれか 1 つのテーブルのポリシーとマッチングされます。マッチングは、受信者のアドレスまたは送信者のアドレスのいずれかに基づいて行われます。

- 受信者アドレスは、エンベロープ受信者アドレスとマッチングされます。  
受信者アドレスのマッチングでは、入力される受信者アドレスは、電子メールパイプラインの先行部による処理後の最後のアドレスです。たとえば、イネーブルにされている場合、デフォルト ドメイン、LDAP ルーティングまたはマスカレード、エイリアス テーブル、ドメイン マップおよびメッセージ フィルタ機能は、エンベロープ受信者アドレスを再作成できます。これにより、電子メール セキュリティ マネージャ（アンチスパム、アンチウイルス、コンテンツ フィルタおよびウイルス感染フィルタ）のポリシーとのメッセージのマッチングに影響を与えることがあります。
- 送信者アドレスは、次のアドレスとマッチングされます。
  - エンベロープ送信者 (RFC821 MAIL FROM アドレス)
  - RFC822 From: ヘッダーのアドレス
  - RFC822 Reply-To: ヘッダーのアドレス

アドレス マッチングは、完全な電子メール アドレス、ユーザ、ドメインまたは部分的なドメインのいずれか、あるいは LDAP グループ メンバーシップで行われます。

## First Match Wins

各受信者は、該当するテーブル（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。

メッセージの各受信者に対して、最初に一致したポリシーが適用されます。受信者がいずれのポリシーにも一致しない場合、その受信者には、自動的に、テーブルのデフォルト ポリシーが適用されます。

マッチングが送信者アドレス（またはアップグレードにより作成される特殊な「リスナー」ルール（以下を参照））に基づいて行われる場合、メッセージの残りの受信者全員に、そのポリシーが適用されます（これは、メッセージごとに存在する送信者またはリスナーが 1 人だけのためです）。

## ポリシー マッチングの例

次の例では、ポリシー テーブルがどのように上から順にマッチングされるかを説明します。

次の表 6-1 に示す着信メールの電子メール セキュリティ ポリシーの表では、着信メッセージはさまざまなポリシーとマッチングされます。

**表 6-1**                    **ポリシー マッチングの例**

順序	ポリシー名	ユーザ
1	special_people	受信者 : joe@example.com 受信者 : ann@example.com
2	from_lawyers	送信者 : @lawfirm.com
3	acquired_domains	受信者 : @newdomain.com 受信者 : @anotherexample.com
4	engineering	受信者 : PublicLDAP.ldapgroup: engineers
5	sales_team	受信者 : jim@ 受信者 : john@ 受信者 : larry@
	Default Policy	(全ユーザ)

## 例 1

送信者 `bill@lawfirm.com` から受信者 `jim@example.com` に送信されるメッセージには、ポリシー 2 が適用されます。これは、表内で、送信者 (`@lawfirm.com`) と一致するユーザ説明が、受信者 (`jim@`) と一致するユーザ説明よりも前に示されているためです。

## 例 2

送信者 `joe@yahoo.com` は、3 人の受信者、`john@example.com`、`jane@newdomain.com` および `bill@example.com` の着信メッセージを送信します。受信者 `jane@newdomain.com` のメッセージには、ポリシー 3 で定義されているアンチスパム、アンチウイルス、ウイルス感染フィルタおよびコンテンツフィルタが適用されますが、受信者 `john@example.com` のメッセージには、ポリシー 5 で定義されている設定が適用されます。受信者 `bill@example.com` は、エンジニアリング LDAP クエリーと一致しないため、このメッセージには、デフォルト ポリシーで定義されている設定が適用されます。次の例では、受信者が複数あるメッセージでメッセージ分裂がどのように発生するかについて示します。詳細については、「[メッセージ分裂](#)」(P.6-194) を参照してください。

## 例 3

送信者 `bill@lawfirm.com` は、受信者 `ann@example.com` および `larry@example.com` にメッセージを送信します。受信者 `ann@example.com` には、ポリシー 1 で定義されているアンチスパム、アンチウイルス、ウイルス感染フィルタおよびコンテンツ フィルタが適用され、受信者 `larry@example.com` には、ポリシー 2 で定義されているアンチスパム、アンチウイルス、ウイルス感染フィルタおよびコンテンツ フィルタが定義されます。これは、表内で、送信者 (`@lawfirm.com`) が、受信者 (`jim@`) と一致するユーザ説明よりも前に示されているためです。

## メッセージ分裂

インテリジェントなメッセージ分裂 (マッチング ポリシーによる) は、受信者が複数あるメッセージに、受信者に基づいた異なるポリシーを個別に適用できるメカニズムです。

各受信者は、該当する電子メール セキュリティ マネージャ 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。

メッセージに一致する各ポリシーは、これらの受信者に新しいメッセージを作成します。このプロセスが、「メッセージ分裂」と定義されます。

- 一部の受信者が異なるポリシーと一致する場合、受信者は一致したポリシーに基づいてグループ化され、メッセージは一致したポリシー数と同数のメッセージに分裂されます。これらの受信者は、それぞれ適切な「分裂先」に設定されます。
- すべての受信者が同じポリシーと一致する場合、メッセージは分裂されません。反対に、最も多くの分裂が行われるのは、単一のメッセージがメッセージ受信者 1 人 1 人に分裂される場合です。
- 各メッセージ分裂は、アンチスパム、アンチウイルス、DLP スキャン、ウイルス感染フィルタおよびコンテンツ フィルタにより、電子メールパイプラインで個別に処理されます。

表 6-2 に、電子メールパイプラインでメッセージが分裂されるポイントを示します。







(注)

---

Email DLP スキャンは、発信メッセージだけで使用できます。

---

表 6-2 電子メール パイプラインでのメッセージ分裂

ワークキュー	メッセージ フィルタ (filters)	電子メールセキュリティマネージャ	↓  すべての受信者のメッセージ
	アンチスパム (antispamconfig, listenerconfig -> antispam)		メッセージは、メッセージ フィルタ処理の直後からアンチスパム処理の前に分裂されます。
	アンチウイルス (antivirusconfig, antivirusupdate listenerconfig -> antivirus)		 すべての受信者のメッセージ ポリシー 1 と一致
	コンテンツ フィルタ (policyconfig -> filters)		 すべての受信者のメッセージ ポリシー 2 と一致
	ウイルス感染フィルタ (vofconfig, vofflush, vofstatus)		 その他のすべての受信者のメッセージ (デフォルト ポリシーと一致)
	データ消失防止 (policyconfig)		



(注)

新しい MID (メッセージ ID) が、各メッセージ分裂用に作成されます (たとえば、MID 1 は、MID 2 および MID 3 になります)。詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Logging」の章を参照してください。また、トレース機能は、メッセージを分裂したポリシーを示します。

電子メールセキュリティマネージャ ポリシーのポリシー マッチングおよびメッセージ分裂は、アプライアンスで使用できるメッセージ処理の管理に影響を与えます。

## 管理例外

分裂メッセージごとの反復処理はパフォーマンスに影響を与えるため、IronPort は、電子メールセキュリティマネージャの着信および発信メール ポリシー テーブルを使用して、*管理例外*単位でポリシーを設定することを推奨します。つまり、組織のニーズを評価し、大多数のメッセージがデフォルト ポリシーで処理され、少数のメッセージが、追加の「例外」ポリシーで処理されるように機能を



設定します。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。

## ポリシーの内容

電子メール セキュリティ マネージャ テーブルは、ユーザの特定のグループ（エンベロープ受信者、エンベロープ送信者、From: ヘッダーまたは Reply-To: ヘッダー）に対して着信または発信メッセージをマッチングし、これらを次の機能の特定の設定にマッピングします。

- アンチスパム スキャン：これらの設定は、旧リリースの AsyncOS のリスナー単位の設定と同じ設定です。詳細については、「[アンチスパム \(P.8-259\)](#)」を参照してください。
- アンチウイルス スキャン：これらの設定は、旧リリースの AsyncOS のリスナー単位の設定と同じ設定です。詳細については、「[アンチウイルス \(P.9-303\)](#)」を参照してください。
- コンテンツ フィルタ：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。
- ウイルス感染フィルタ

IronPort のウイルス感染フィルタ機能は、従来のアンチウイルス セキュリティ サービスが新しいウイルス シグニチャ ファイルで更新されるまで、疑わしいメッセージを検疫することで、新種ウイルスの発生に対する「第一の防衛ライン」を提供する予測セキュリティ サービスです。ウイルス感染フィルタは特定の受信者に対してイネーブルまたはディセーブルにできません。また、電子メール セキュリティ マネージャのウイルス感染フィルタ機能をバイパスするファイルタイプを定義することもできます。詳細については、[第 10 章「ウイルス感染フィルタ」](#)を参照してください。

- データ消失防止：詳細については、[第 11 章「データ消失防止」](#)を参照してください。

**図 6-1** に、ポリシーで定義されたユーザを特定のアンチスパム、アンチウイルス、ウイルス感染フィルタ、DLP およびコンテンツ フィルタ設定にマッピングする GUI の電子メール セキュリティ マネージャを示します。

図 6-1 GUI の電子メール セキュリティ マネージャ ポリシーの概要  
Incoming Mail Policies

Find Policies

Email Address: 

 Recipient  
 Sender
 
Find Policies

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Virus Outbreak Filters	Content Filters	Delete
1	Sales_Team	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	(use default)	(use default)	drop_large_attachments ex_employee no_mp3s scan_for_confidential	🗑️
2	Engineering	(use default)	(use default)	Enabled	ex_employee scan_for_confidential	🗑️
	Default Policy	IronPort Anti-Spam Positive: Deliver Suspected: Disabled	Repaired: Deliver Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Enabled	ex_employee no_mp3s scan_for_confidential	

Key: Default Custom Disabled

## コンテンツ フィルタの概要

電子メール セキュリティ マネージャ ポリシーでは、受信者または送信者単位でメッセージに適用されるコンテンツ フィルタを作成できます。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、1 つのメッセージが、各電子メール セキュリティ マネージャ 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 フィルタ機能は、メッセージ フィルタ処理およびアンチスパムとアンチウイルス スキャンがメッセージに対して実行された後で適用されます。

通常メッセージ フィルタと同様に、各コンテンツ フィルタに名前を定義します。この名前は、使用される着信または発信メール ポリシー テーブルで一意でなければなりません。各着信および発信メール ポリシー テーブルには、コンテンツ フィルタ独自の単一「マスター リスト」があります。順序は、テーブル単位（着信または発信）で定義されます。ただし、各個別のポリシーは、実行される特定のフィルタを決定します。

通常メッセージ フィルタ（アンチスパムおよびアンチウイルス スキャンの前に適用される）とは異なり、コンテンツ フィルタは、CLI および GUI の両方で設定できます。GUI には、「ルール ビルダ」ページがあります。このページで

は、コンテンツ フィルタを構成する条件およびアクションを簡単に作成できます。電子メール セキュリティ マネージャの着信または発信メール ポリシー テーブルは、特定のポリシーに適用される順序で、イネーブルにされるコンテンツ フィルタを管理します。表 6-3 に、コンテンツ フィルタの作成に使用できる条件を示します。表 6-4 に、コンテンツ フィルタの定義に使用できる非最終および最終アクションを示します。コンテンツ フィルタは、条件およびアクションにより構成されます。表 6-5 に、コンテンツ フィルタの作成に使用できるアクション変数を示します。

## コンテンツ フィルタの条件

コンテンツ フィルタでの条件の指定はオプションです。

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場合、メッセージおよび添付ファイルで検出する一致数の「スコア」を合計します。最小しきい値が満たされていない場合、正規表現は `true` に評価されません。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。

また、「スマート ID」を使用して、データのパターンを識別することもできます。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

パターンが検出される回数の最小しきい値の指定、およびスマート ID の詳細については、『*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。

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」）のいずれかで結合するかを選択できます。

表 6-3 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 ルールが適用されず、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。
[Message Body or Attachments]	<p>[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。</p> <p>[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。</p> <p>[Contains term in content dictionary] : メッセージ本文に、&lt;dictionary name&gt; 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。</p> <p>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。「<a href="#">コンテンツ ディクショナリ</a>」(P.14-431) を参照してください。</p> <p>[Number of matches required] : ルールが true と評価されるために必要な一致回数を指定します。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。</p> <p>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。</p>

表 6-3 コンテンツ フィルタの条件 (続き)

条件	説明
[Message Body]	<p>[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。</p> <p>[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。</p> <p>[Contains term in content dictionary] : メッセージ本文に、&lt;dictionary name&gt; 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。</p> <p>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。「<a href="#">コンテンツ ディクショナリ</a>」(P.14-431) を参照してください。</p> <p>[Number of matches required] : ルールが true と評価されるために必要な一致回数を指定します。このしきい値は、テキストまたはスマート ID に指定できます。</p> <p>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。</p>
[Message Size]	<p>本文サイズが、指定範囲内にあるかどうかを判別します。本文サイズは、ヘッダーと添付ファイルの両方を含む、メッセージのサイズを示します。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。</p>

表 6-3 コンテンツ フィルタの条件 (続き)

条件	説明
<b>[Attachment Content]</b>	<p>[Contains text] : メッセージに、特定の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含まれている添付ファイルが関連付けられているかどうかを判別します。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。</p> <p>[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。</p> <p>[Contains terms in content dictionary] : 添付ファイルに、&lt;dictionary name&gt; 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。</p> <p>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。<a href="#">「コンテンツ ディクショナリ」 (P.14-431)</a> を参照してください。</p> <p>[Number of matches required] : ルールが true と評価されるために必要な一致回数を指定します。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。</p>

表 6-3 コンテンツ フィルタの条件 (続き)

条件	説明
<b>[Attachment File Info]</b>	<p>[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含まれているかどうかを判別します。</p> <p>[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含まれているかどうかを判別します (UNIX file コマンドと似ています)。</p> <p>[MIME type] : メッセージに、特定の MIME タイプの添付ファイルが含まれているかどうかを判別します。このルールは、attachment-type ルールと似ていますが、このルールでは、MIME 添付ファイルにより指定される MIME タイプだけが評価されます (アプライアンスは、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)。</p> <p>[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含まれているかどうかを判別します。有効なイメージ分析判定には、[Suspect]、[Inappropriate]、[Suspect or Inappropriate]、[Unscannable] または [Clean] があります。</p>
<b>[Attachment Protection]</b>	<p>[Contains an attachment that is password-protected or encrypted] :</p> <p>(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)</p> <p>[Contains an attachment that is NOT password-protected or encrypted] :</p> <p>(この条件は、たとえば、すべての添付ファイルが暗号化されているかを確認するために、Encrypt アクションとともに使用します)</p>

表 6-3 コンテンツ フィルタの条件 (続き)

条件	説明
[Subject Header]	<p>[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。</p> <p>[Contains terms in content dictionary] : 件名ヘッダーに、&lt;<i>dictionary name</i>&gt; という名前のコンテンツ デictionary 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。</p> <p>Dictionary用語を検索するには、Dictionaryがすでに作成されている必要があります。「<a href="#">コンテンツ Dictionary</a>」 (P.14-431) を参照してください。</p>
[Other Header]	<p>[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。</p> <p>[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。</p> <p>ヘッダーの値には、コンテンツ Dictionaryの用語が含まれます。指定されたヘッダーに、&lt;<i>dictionary name</i>&gt; という名前のコンテンツ Dictionary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。</p> <p>Dictionary用語を検索するには、Dictionaryがすでに作成されている必要があります。「<a href="#">コンテンツ Dictionary</a>」 (P.14-431) を参照してください。</p>



表 6-3 コンテンツ フィルタの条件 (続き)

条件	説明
<b>[Envelope Sender]</b>	<p>[Envelope Sender] : エンベロープ送信者 (つまり、Envelope From、&lt;MAIL FROM&gt;) が、特定のパターンと一致するかどうかを判別します。</p> <p>[Matches LDAP group] : エンベロープ送信者 (つまり、Envelope From、&lt;MAIL FROM&gt;) が、特定の LDAP グループに含まれるかどうかを判別します。</p> <p>[Contains term in content dictionary] : エンベロープ送信者に、&lt;dictionary name&gt; 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。</p> <p>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。「<a href="#">コンテンツ ディクショナリ</a>」(P.14-431) を参照してください。</p>

表 6-3 コンテンツ フィルタの条件 (続き)

条件	説明
[Envelope Recipient]	<p>[Envelope Recipient] : エンベロープ受信者 (つまり、Envelope To、&lt;RCPT TO&gt;) が、特定のパターンと一致するかどうかを判別します。</p> <p>[Matches LDAP group] : エンベロープ受信者 (つまり、Envelope To、&lt;RCPT TO&gt;) が、特定の LDAP グループに含まれるかどうかを判別します。</p> <p>[Contains term in content dictionary] : エンベロープ受信者に、&lt;dictionary name&gt; 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。</p> <p>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。「<a href="#">コンテンツ ディクショナリ</a>」(P.14-431) を参照してください。</p> <p><b>注 :</b> [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 人だけ検出されれば、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。</p> <p>エンベロープ送信者 (つまり、Envelope From、&lt;MAIL FROM&gt;) が、特定の LDAP グループに含まれるかどうかを判別します。</p>
[Receiving Listener]	<p>メッセージが、指定されたリスナーを介して着信したかどうかを判別します。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なければなりません。</p>

表 6-3 コンテンツ フィルタの条件 (続き)

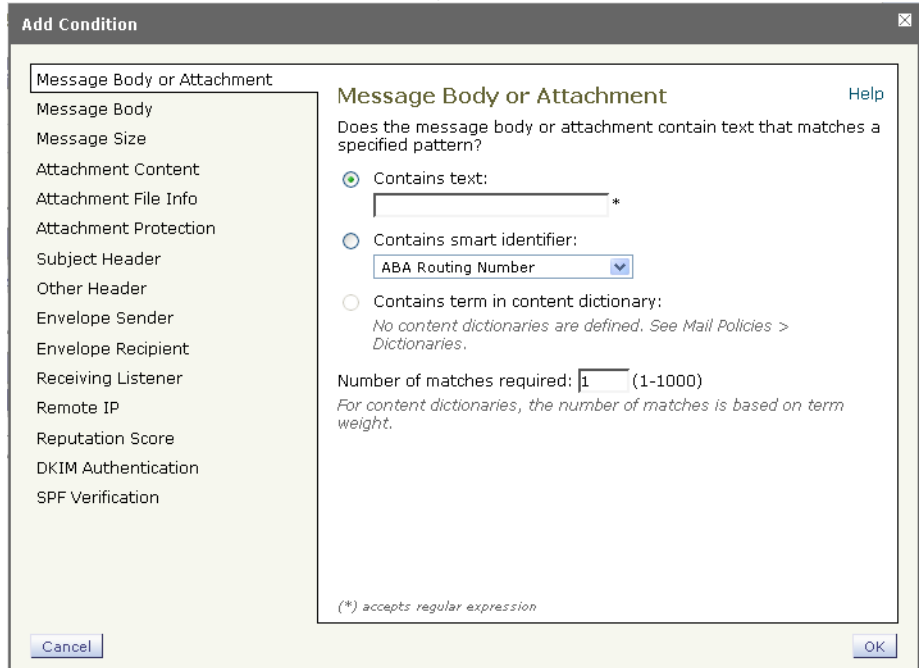
条件	説明
[Remote IP]	メッセージが、特定の IP アドレスまたは IP ブロックと一致するリモート ホストから送信されたかどうかを判別します。[Remote IP] ルールは、メッセージを送信したホストの IP アドレスが特定のパターンと一致するかどうかをテストします。IP アドレス パターンは、「送信者グループの構文」(P.5-132) で説明されている、許可されたホスト表記を使用して指定されます。ただし、SBO、SBRs、dnstlist 表記および特殊キーワード ALL を除きます。
[Reputation Score]	送信者の SenderBase 評価スコアを検証します。[Reputation Score] は、別の値に対する SenderBase 評価スコアをチェックします。
[DKIM Authentication]	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。
[SPF Verification]	SPF 検証ステータスを判別します。このフィルタでは、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、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Email Authentication」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なっ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」(P.14-431) を参照してください。

図 6-2 コンテンツ フィルタの条件



## コンテンツ フィルタのアクション

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 or Attachment] 条件、[Message Body] 条件または [Attachment Content] 条件に一致するメッセージの検疫アクションを設定する場合は、検疫されたメッセージの一致した内容を表示できます。メッセージの本文を表示する場合、一致した内容は、黄色で強調表示されません。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、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』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。

表 6-4 コンテンツ フィルタのアクション

アクション	説明
<b>[Quarantine]</b>	<p>[Quarantine] : いずれかのシステム検疫エリアに保持されるメッセージにフラグを付けます。</p> <p>[Duplicate message] : メッセージのコピーを指定された検疫エリアに送信して、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。</p>
<b>[Encrypt on Delivery]</b>	<p>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。</p> <p>[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、「<a href="#">TLS 接続を暗号化の代わりに使用</a>」(P.12-407) を参照してください。</p> <p>[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、IronPort 暗号化アプライアンスまたはホステッドキー サービスで使用されます。</p> <p>[Subject] : 暗号化されたメッセージの件名です。デフォルトでは、この値は、\$Subject です。</p>

表 6-4 コンテンツ フィルタのアクション (続き)

アクション	説明
<b>[Strip Attachment by Content]</b>	<p>[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、それらに含まれる任意のファイルが、正規表現パターンと一致した場合にドロップされます。</p> <p>[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。</p> <p>[Attachment contains terms in the content dictionary] : 添付ファイルに、&lt;dictionary name&gt; 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。</p> <p>[Number of matches required] : ルールが true と評価されるために必要な一致回数を指定します。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。</p> <p>[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。メッセージに、添付ファイル フッターが追加されます。</p>

表 6-4 コンテンツ フィルタのアクション (続き)

アクション	説明
<b>[Strip Attachment by File Info]</b>	<p>[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 ファイルの添付ファイル (zip、tar) は、それらに含まれるファイルが一致した場合にドロップされません。</p> <p>[File size] : ロー エンコード形式で、指定サイズ (バイト単位) 以上の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、実際の添付ファイルのサイズを検証するため注意してください。</p> <p>[File type] : ファイルの指定「フィンガープリント」と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 ファイルの添付ファイル (zip、tar) は、それらに含まれるファイルが一致した場合にドロップされます。</p> <p>[MIME type] : タイプが指定 MIME タイプであ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。</p> <p>[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、[Suspect]、[Inappropriate]、[Suspect or Inappropriate]、[Unscannable] または [Clean] があります。</p> <p>[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。メッセージに、添付ファイル フッターが追加されます。</p>

表 6-4 コンテンツ フィルタのアクション (続き)

アクション	説明
<b>[Add Disclaimer Text]</b>	<p>[Above] : メッセージ上部に免責事項を追加します (ヘッダー)。</p> <p>[Below] : メッセージ下部に免責事項を追加します (フッター)。</p> <p>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。</p> <p>詳細については、「免責事項テキスト」(P.14-452) を参照してください。</p>
<b>[Bypass Outbreak Filter Scanning]</b>	このメッセージのウイルス感染フィルタ スキャンをバイパスします。
<b>[Send Copy (Bcc:)]</b>	<p>[Email addresses] : 指定受信者にメッセージを匿名でコピーします。</p> <p>[Subject] : コピーされたメッセージの件名を追加します。</p> <p>[Return path (optional)] : リターン パスを指定します。</p> <p>[Alternate mail host (optional)] : 代替メール ホストを指定します。</p>



表 6-4 コンテンツ フィルタのアクション (続き)

アクション	説明
<b>[Notify]</b>	<p><b>通知。</b> 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。</p> <p>[Subject] : コピーされたメッセージの件名を追加します。</p> <p>[Return path (optional)] : リターン パスを指定します。</p> <p>[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。</p> <p>[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。</p>
<b>[Change Recipient to]</b>	[Email address] : 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。
<b>[Send to Alternate Destination Host]</b>	<p>[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。</p> <p>(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検疫されないようにします。このアクションは、検疫を無効にして、指定メール ホストに送信します。</p>
<b>[Deliver from IP Interface]</b>	[Send from IP interface] : 指定 IP インターフェイスから送信します。[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。
<b>[Strip Header]</b>	[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。

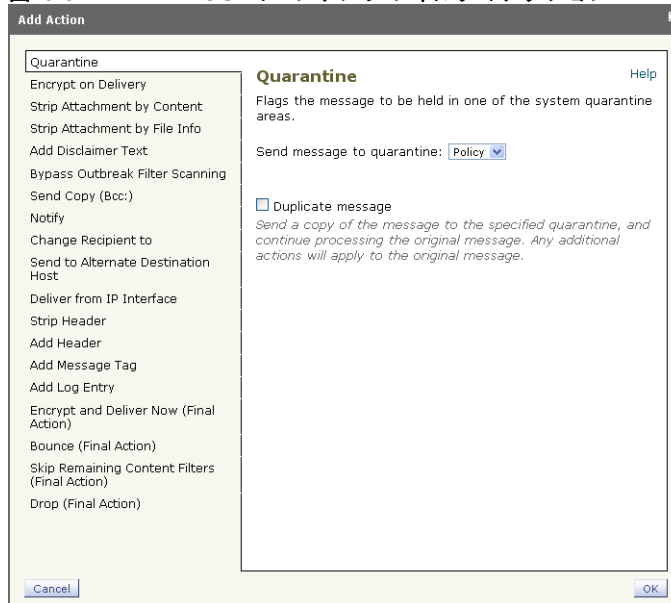
表 6-4 コンテンツ フィルタのアクション (続き)

アクション	説明
[Add Header]	<p>[Header name] : ヘッダーを配信前にメッセージに挿入します。</p> <p>[Header value] : ヘッダーの値を配信前にメッセージに挿入します。</p>
[Add Message Tag]	<p>RSA Email 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。RSA Email DLP ポリシーを設定して、スキャンをメッセージ タグの付いたメッセージに制限できます。メッセージ タグは、受信者に表示されません。DLP ポリシーでのメッセージ タグの使用については、「<a href="#">DLP ポリシー</a>」(P.11-366) を参照してください。</p>
[Add Log Entry]	<p>カスタマイズされたテキストを INFO レベルで IronPort Text Mail ログに挿入します。テキストには、アクション変数を含めることができます。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。</p>
[Encrypt and Deliver Now (Final Action)]	<p>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。</p> <p>[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、「<a href="#">TLS 接続を暗号化の代わりに使用</a>」(P.12-407) を参照してください。</p> <p>[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、IronPort 暗号化アプライアンスまたはホステッド キー サービスで使用されます。</p> <p>[Subject] : 暗号化されたメッセージの件名です。デフォルトでは、この値は、\$Subject です。</p>
[Bounce (Final Action)]	<p>メッセージを送信者に戻します。</p>

表 6-4 コンテンツ フィルタのアクション (続き)

アクション	説明
<b>[Skip Remaining Content Filters (Final Action)]</b>	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、検疫が実行されるか、感染フィルタによるスキャンが開始されます。
<b>[Drop (Final Action)]</b>	メッセージをドロップして廃棄します。

図 6-3 GUI のコンテンツ フィルタのアクション



## 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。これらの特殊変数は、アクション変数と呼ばれます。IronPort アプライアンスでは、次のアクション変数のセットをサポートしています。

表 6-5 アクション変数

変数	構文	説明
<b>All Headers</b>	\$AllHeaders	メッセージ ヘッダーに置き換えられます。
<b>Body Size</b>	\$BodySize	メッセージのサイズ (バイト単位) に置き換えられます。
<b>Date</b>	\$Date	現在の日付 (MM/DD/YYYY 形式) に置き換えられます。
<b>Dropped File Name</b>	\$dropped_filename	直前にドロップされたファイル名のみを返します。
<b>Dropped File Names</b>	\$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。
<b>Dropped File Types</b>	\$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。
<b>Envelope Sender</b>	\$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。
<b>Envelope Recipients</b>	\$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。
<b>File Names</b>	\$filenames	メッセージの添付ファイルのファイル名を示すカンマ区切りリストに置き換えられます。
<b>File Sizes</b>	\$filesizes	メッセージの添付ファイルのファイルサイズを示すカンマ区切りリストに置き換えられます。

表 6-5 アクション変数 (続き)

変数	構文	説明
<b>File Types</b>	\$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。
<b>Filter Name</b>	\$FilterName	処理されるフィルタの名前に置き換えられます。
<b>GMTimeStamp</b>	\$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 <b>Received:</b> 行で見られる形式と同様です。
<b>HAT Group Name</b>	\$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。
<b>Mail Flow Policy</b>	\$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。
<b>Matched Content</b>	\$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。Matched Content は、コンテンツ ディクショナリ マッチング、スマート ID または正規表現マッチングにすることができます。
<b>Header</b>	\$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。二重引用符も使用できるため注意してください。
<b>Hostname</b>	\$Hostname	IronPort アプライアンスのホスト名に置き換えられます。

表 6-5 アクション変数 (続き)

変数	構文	説明
<b>Internal Message ID</b>	\$MID	メッセージを識別するために内部的に使用されるメッセージ ID または「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)。
<b>Receiving Listener</b>	\$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。
<b>Receiving Interface</b>	\$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。
<b>Remote IP Address</b>	\$RemoteIP	メッセージを IronPort アプライアンスに送信したシステム IP アドレスに置き換えられます。
<b>Remote Host Address</b>	\$remotehost	メッセージを IronPort アプライアンスに送信したシステムのホスト名に置き換えられます。
<b>SenderBase Reputation Score</b>	\$Reputation	送信者の SenderBase 評価スコアに置き換えられます。評価スコアがない場合、「None」に置き換えられます。
<b>Subject</b>	\$Subject	メッセージの件名に置き換えられます。
<b>Time</b>	\$Time	現在の時刻 (ローカル時間帯) に置き換えられます。
<b>Timestamp</b>	\$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。

## 実際の例 (GUI)

この例では、次のタスクを示し、電子メール セキュリティ マネージャの機能について説明します。

- ステップ 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、ウイルス感染フィルタおよびコンテンツ フィルタを編集します。
- ステップ 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。
- ステップ 3** [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。
- ステップ 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電子メール セキュリティ マネージャのアンチスパム、アンチウイルス、ウイルス感染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。アンチスパム、アンチウイルスおよびウイルス感染フィルタの機能の詳細については、次の章を参照してください。

- 「アンチスパム」 (P.8-259)
- 「アンチウイルス」 (P.9-303)
- 「ウイルス感染フィルタ」 (P.10-335)

## 電子メール セキュリティ マネージャへのアクセス

新しくインストールされた、またはアップグレードされたシステムでは、[Mail Policies] タブをクリックして、電子メール セキュリティ マネージャにアクセスします。デフォルトでは、[Incoming Mail Policies] テーブルが表示されます。

新規システムでは、System Setup Wizard のすべての手順を完了して、IronPort Anti-Spam、Sophos または McAfee Anti-Virus およびウイルス感染フィルタをイネーブルにするように選択した場合、[図 6-4](#) のような [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 (IronPort スпам検疫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：検疫、メッセージの件名が追加
  - 陽性と疑わしいスパム：検疫、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 (IronPort スпам検疫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
- ウイルス感染フィルタ：イネーブル
  - ファイル拡張子は予測されない
- コンテンツ フィルタ：ディセーブル

図 6-4 [Incoming Mail Policies] ページ：新規アプライアンスのデフォルト Incoming Mail Policies

Find Policies						
Email Address:		<input type="text"/>	<input checked="" type="radio"/> Recipient <input type="radio"/> Sender	<input type="button" value="Find Policies"/>		
Policies						
<input type="button" value="Add Policy..."/>						
Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine Marketing Messages: Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Enabled	

Key:



(注)

この例では、着信メール ポリシーは、IronPort スпам検疫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。



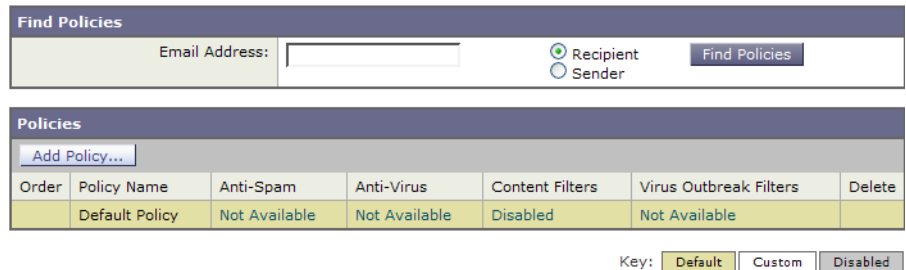
## [Enabled]、[Disabled]、[Not Available]

[Email Security Manager] 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、単語 [Enabled] 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、単語 [Disabled] 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 [Not Available] が表示されます。この場合、[Not Available] リンクをクリックすると、[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。

図 6-5 を参照してください。

図 6-5 使用できないセキュリティ サービス  
Incoming Mail Policies



Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
	Default Policy	Not Available	Not Available	Disabled	Not Available	

Key: Default Custom Disabled

## デフォルト ポリシーの編集：アンチスパム設定

電子メール セキュリティ マネージャの各行は、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、電子メール セキュリティ マネージャの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。

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 メッセージが検疫され、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検疫されます。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。

**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。図 6-6 に示す [Anti-Spam Settings] ページが表示されます。



**(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。[Disable] をクリックして、サービスをディセーブルにできます。

**ステップ 2** [Positively Identified Spam Settings] セクションでは、[Action to apply to this message] を [Drop] に変更します。

**ステップ 3** [Marketing Email Settings] セクションでは、[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。

[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** [Submit] をクリックします。[Incoming Mail Policies table] ページが再表示されます。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感染フィルタ設定を変更できます。

図 6-6 [Anti-Spam Settings] ページ  
Mail Policies: Anti-Spam

Anti-Spam Settings	
Policy:	Default
Enable Anti-Spam Scanning for This Policy:	<input checked="" type="radio"/> Use IronPort Anti-Spam service <input type="radio"/> Disabled
Positively-Identified Spam Settings	
Apply This Action to Message:	Drop
Add Text to Subject:	Prepend [SPAM]
Advanced Optional settings for custom header and message delivery.	
Suspected Spam Settings	
Enable Suspected Spam Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Spam Quarantine
Note: If local and external quarantines are defined, mail will be sent to local quarantine.	
Add Text to Subject:	Prepend [SUSPECTED SPAM]
Advanced Optional settings for custom header and message delivery.	
Marketing Email Settings	
Enable Marketing Email Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Deliver
Send to Alternate Host (optional):	
Add Text to Subject:	Prepend [MARKETING]
Advanced Optional settings for custom header and message delivery.	
Spam Thresholds	
Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.	
IronPort Anti-Spam:	<input checked="" type="radio"/> Use the Default Thresholds <input type="radio"/> Use Custom Settings:
Positively Identified Spam: Score > 90 (50 - 100)	
Suspected Spam: Score > 50 (minimum 25, cannot exceed positive spam score)	
Cancel	Submit

## 新しいポリシーの作成

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。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。

**ステップ 1** [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。

[Add Users] ページが表示されます。

**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。詳細については、「[First Match Wins](#)」(P.6-193) を参照してください。

### ステップ 3 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](#)」(P.6-192) を参照してください）。[図 6-7](#) 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。ポリシーのユーザを入力する場合は注意してください。たとえば、ユーザの受信者 Joe@ を入力した場合、joe@example.com に送信されるメッセージは一致しません。

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、IronPort アプライアンスを設定して、LDAP サーバをクエリーし、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、電子メール セキュリティ マネージャのメール ポリシーのユーザを定義できます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の章を参照してください。

図 6-7 ポリシーのユーザの定義  
Add Incoming Mail Policy

**ステップ 4** [Add] ボタンをクリックして、[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ることができます。

[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 5** ユーザの追加が完了したら、[Submit] をクリックします。

新しいポリシーが追加された状態で [Mail Policies] ページが表示されます。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 6-8 新しく追加されたポリシー：販売グループ

Policies						
Add Policy...						
Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	Sales_Team	(use default)	(use default)	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Enabled	

Key:  Default  Custom  Disabled

**ステップ 6** [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 6-9 エンジニアリング チームのポリシーの作成**  
**Add Incoming Mail Policy**

**ステップ 7** 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、[Submit] をクリックします。

新しいポリシーが追加された状態で [Mail Policies] ページが表示されます。

[図 6-10](#) を参照してください。

**ステップ 8** 変更を確定します。

**図 6-10 新しく追加されたポリシー : エンジニアリング チーム**

Policies						
Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	Sales_Team	(use default)	(use default)	(use default)	(use default)	
2	Engineering	(use default)	(use default)	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Enabled	

Key:  Default  Custom  Disabled

**(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。

## [Default]、[Custom]、[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。

Key: Default Custom Disabled

- 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。

## カスタム 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（「[デフォルト ポリシーの編集：アンチスパム設定](#)」(P.6-221) 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、IronPort スパム検疫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、「[アンチスパム](#)」(P.8-259) を参照してください。

- エンジニアリング チームでは、拡張子「dwg」のファイルがウイルス感染フィルタのスキャンをバイパスするように、ウイルス感染フィルタ機能の設定をカスタマイズします。

ウイルス感染フィルタの設定の詳細については、「[ウイルス感染フィルタ \(P.10-335\)](#)」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。

- 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 ([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 [(use default)] です。

**図 6-11 販売チーム ポリシーのアンチスパム設定の編集**

Policies		
Add Policy...		
Order	Policy Name	Anti-Spam
1	Sales_Team	(use default)
2	Engineering	(use default)
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Deliver

アンチスパムの設定ページが表示されます。

- 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、[Enable Anti-Spam Scanning for this Policy] の値を [Use Default Settings] から [Use IronPort Anti-Spam] に変更します。

[Use IronPort Anti-Spam] 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** [Positively-Identified Spam Settings] セクションで、[Apply This Action to Message] を [Drop] に変更します。

- ステップ 4** [Suspected Spam Settings] セクションで、[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** [Suspected Spam Settings] セクションで、[Apply This Action to Message] を [Spam Quarantine] に変更します。





(注) [IronPort Spam Quarantine] を選択すると、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Quarantines」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** [Add text to subject] フィールドで、[None] をクリックします。
- IronPort スпам検疫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** [Marketing Email Settings] セクションで、[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** [Apply This Action to Message] セクションで、[Spam Quarantine] を選択します。
- ステップ 9** 変更を送信して確定します。

販売ポリシーの変更が反映された状態で、[Incoming Mail Policies] ページが表示されます。図 6-12 を参照してください。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。

図 6-12 変更された販売グループのポリシーのアンチスパム設定

Policies		
Add Policy...		
Order	Policy Name	Anti-Spam
1	Sales_Team	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Quarantine
2	Engineering	(use default)
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Deliver

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пам検疫エリアに配信されます。

エンジニアリング チーム ポリシーのウイルス感染フィルタ設定を編集するには、次の手順を実行します。

- ステップ 1** エンジニアリング ポリシー行のウイルス感染フィルタ機能セキュリティ サービス ([Virus 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 [(use default)] です。

図 6-13 エンジニアリング チーム ポリシーのウイルス感染フィルタ機能設定の編集

Policies						
Add Policy...						
Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	Sales_Team	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Quarantine	(use default)	(use default)	(use default)	
2	Engineering	(use default)	(use default)	(use default)	<a href="#">(use default)</a>	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Enabled	

Key:  Default  Custom  Disabled

**ステップ 2** [Virus Outbreak Filters feature security service] ページで、[Enable Virus Outbreak Filter Scanning for this Policy] の値を [Use Default Settings] から [Yes] に変更します。

[Yes] 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 [Bypass Outbreak Filtering For] 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。

ファイル拡張子「dwg」は、IronPort アプライアンスが添付ファイルのスクリー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** [Add Extension] をクリックして、.dwg ファイルをウイルス感染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。

図 6-14 ウイルス感染フィルタのバイパス  
Mail Policies: Virus Outbreak Filters

**ステップ 5** 変更を送信して確定します。

エンジニアリング ポリシーの変更が反映された状態で、[Incoming Mail Policies] ページが表示されます。図 6-15 を参照してください。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。

図 6-15 変更された販売チームのポリシーのアンチスパム設定

Policies						
Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	Sales_Team	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Quarantine	(use default)	(use default)	(use default)	
2	Engineering	(use default)	(use default)	(use default)	Enabled	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Enabled	

Key: Default Custom Disabled

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、ウイルス感染フィルタ スキャンをバイパスし、処理を続行します。

## 電子メール セキュリティ マネージャのポリシーのユーザの検索

[Find Policies] ボタンを使用して、[Email Security Manager Incoming] または [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、[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。

図 6-16 ポリシーでのユーザの検索

The screenshot shows the 'Find Policies' interface. At the top, there is a search bar with 'Email Address: joe@example.com' and radio buttons for 'Recipient' (selected) and 'Sender'. A 'Find Policies' button is to the right. Below this, the results section shows: 'Results: Email Address "Recipient: joe@example.com" is defined in the following policies: Engineering, Default Policy (all users)'. Below the results is a table titled 'Policies matching "joe@example.com"'. The table has columns: Order, Policy Name, Anti-Spam, Anti-Virus, Content Filters, Virus Outbreak Filters, and Delete. The 'Engineering' policy is selected, showing details for Anti-Spam, Anti-Virus, Content Filters, and Virus Outbreak Filters. A 'Key:' section at the bottom right shows 'Default' (selected), 'Custom', and 'Disabled'.

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
2	Engineering	(use default)	(use default)	(use default)	Enabled	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Enabled	

Key:  Default  Custom  Disabled

ポリシーの名前をクリックして、[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。

## 電子メール セキュリティ マネージャ : 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。表 6-6 (P.6-233) に、ポリシーの例をいくつか示します。「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、false positive 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 6-6 積極的および保守的な電子メール セキュリティ マネージャ設定

	積極的な設定	保守的な設定
アンチスパム	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：検疫 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：検疫 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
アンチウイルス	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：検疫 スキャンできないメッセージ：検疫 感染メッセージ：ドロップ
ウイルス拡散防止フィルタ	イネーブル、バイパスできるファイル名拡張子なし	イネーブル、特定のファイル名拡張子がバイパス可能

## 新しいコンテンツ フィルタの作成

この例では、[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。次のフィルタを作成します。

### ステップ 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。文字列が見つかったら、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 Policy 検疫エリアに送信されます。

### ステップ 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。

**ステップ 3** 「ex\_employee」

このコンテンツ フィルタは、特定のエンベロップ受信者アドレス（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。

**Confidential のスキャン**

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。コンテンツ フィルタを作成するには、次の手順を実行します。

**ステップ 1** [Mail Policies] タブをクリックします。

**ステップ 2** [Incoming Content Filters Section] をクリックします。

[Incoming Content Filters] ページが表示されます。新しくインストールされたシステムまたはアップグレードされたシステムの場合、デフォルトで、コンテンツ フィルタは定義されていません。

**図 6-17** [Incoming Content Filters] ページ  
**Incoming Content Filters**



**ステップ 3** [Add Filter] ボタンをクリックします。

[Add Content Filter] ページが表示されます。

**ステップ 4** [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** [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 6** [Add Condition] をクリックします。
- ステップ 7** [Message Body] を選択します。
- ステップ 8** [Contains text:] フィールドに `confidential` と入力して、[OK] をクリックします。
- [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 9** [Add Action] をクリックします。
- ステップ 10** [Send Copy To (Bcc:)] を選択します。
- ステップ 11** [Email Addresses] フィールドに、`hr@example.com` と入力します。
- ステップ 12** [Subject] フィールドに、`[message matched confidential filter]` と入力します。
- ステップ 13** [OK] をクリックします。
- [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 14** [Add Action] をクリックします。
- ステップ 15** [Quarantine] を選択します。
- ステップ 16** ドロップダウンメニューで、[Policy quarantine area] を選択します。
- ステップ 17** [OK] をクリックします。
- [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 18** 変更を送信して確定します。

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 ポリシーでもイネーブルになっていません。この例では、新しいコンテンツ フィルタをマスター 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、電子メール セキュリティ マネージャ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。

## MP3 添付ファイルなし

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。2 番目のコンテンツ フィルタを作成するには、次の手順を実行します。

- 
- ステップ 1** [Add Filter] ボタンをクリックします。
- [Add Content Filter] ページが表示されます。

- ステップ 2** [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** [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 4** [Add Action] をクリックします。
- ステップ 5** [Strip Attachment by File Info] を選択します。
- ステップ 6** [File type is] を選択します。
- ステップ 7** ドロップダウン フィールドで、`[-- mp3]` を選択します。
- ステップ 8** 必要な場合、置換メッセージを入力します。
- ステップ 9** [OK] をクリックします。

[Add Content] 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 10** 変更を送信して確定します。



(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

3 番めのコンテンツ フィルタを作成するには、次の手順を実行します。

- 
- ステップ 1** [Add Filter] ボタンをクリックします。  
[Add Content Filter] ページが表示されます。
  - ステップ 2** [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** [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 4** [Add Condition] をクリックします。
  - ステップ 5** [Envelope Recipient] を選択します。
  - ステップ 6** エンベロープ受信者に対して、`[Begins with]` を選択して、`doug@` と入力します。



**ステップ 7** [OK] をクリックします。

[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 8** [Add Action] をクリックします。

**ステップ 9** [Notify] を選択します。

**ステップ 10** [Sender] チェックボックスを選択して、[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 11** [Use template] セクションで、通知テンプレートを選擇します。



**(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 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、[Mail Policies] > [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](#)」(P.14-431) を参照してください。

**ステップ 12** [OK] をクリックします。

[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 13** [Add Action] をクリックします。

**ステップ 14** [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、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 15** 変更を送信して確定します。

[Incoming Content Filters] ページが表示され、新しく追加されたコンテンツ フィルタが表示されます。

## 個々のポリシーへのコンテンツ フィルタのイネーブル化および適用

前述の例では、[Incoming Content Filters] 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。[Incoming Content Filters] および [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「マスター リスト」が含まれます。

**図 6-18 [Incoming Content Filters] : 作成された 3 つのフィルタ Incoming Content Filters**

Filters				
<a href="#">Add Filter...</a>				
Order	Filter Name	Description   Rules   Policies	Duplicate	Delete
1	<a href="#">scan_for_confidential</a>	scan all incoming mail for the string 'confidential'		
2	<a href="#">no_mp3s</a>	strip all MP3 attachments		
3	<a href="#">ex_employee</a>	bounce messages intended for Doug		

この例では、[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。

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。デフォルト着信メール ポリシーを編集するには、次の手順を実行します。

**ステップ 1** [Incoming Mail Policies] をクリックして、[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「[新しいポリシーの作成](#)」(P.6-223) 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 ([Content Filters] 列) のリンクをクリックします。図 6-19 を参照してください。

図 6-19 デフォルト着信メール ポリシーのコンテンツ フィルタ設定の編集

Policies						
Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	Sales_Group	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	(use default)	(use default)	(use default)	
2	Engineering	(use default)	(use default)	(use default)	Enabled	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Enabled	

**ステップ 3** [Content Filtering] セキュリティ サービス ページで、[Enable Content Filtering for this Policy] の値を [No] から [Yes] に変更します。

図 6-20 ポリシーでのコンテンツ フィルタのイネーブル化および特定のコンテンツ フィルタの選択

## Mail Policies: Content Filters

Content Filtering for: Default Policy			
Enable Content Filtering for this Policy:			<input checked="" type="radio"/> Yes <input type="radio"/> No
Content Filters			
Order	Filter Name	Description	Enable
1	scan_for_confidential	scan all incoming email for the string "confidential"	<input type="checkbox"/>
2	no_mp3s	strip all mp3 attachments	<input type="checkbox"/>
3	ex_employee	bounce messages intended for Doug	<input type="checkbox"/>
Cancel		Submit	

マスター リストで定義されているコンテンツ 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」(P.6-198) 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 [No] から [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。



**(注)** デフォルトでは、ポリシーのコンテンツ フィルタリングをイネーブルにすると、すべてのコンテンツ フィルタが選択されます。

**ステップ 4** [Submit] をクリックします。

[Incoming Mail Policies] ページが表示され、テーブルが更新され、デフォルト ポリシーでイネーブルにされているフィルタの名前が示されます。

図 6-21 デフォルト着信メール ポリシーでイネーブルにされた 3 つのコンテンツ フィルタ

Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	scan_for_confidential no_mp3s ex_employee
----------------	--	--	---

「エンジニアリング」ポリシーのコンテンツ 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。

- ステップ 1** エンジニアリング チーム ポリシー行の [Content Filters security service] ([Content Filters] 列) のリンクをクリックします。
- ステップ 2** [Content Filtering security service] ページで、[Enable Content Filtering for this Policy] の値を [Use Default Settings] から [Yes] 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 [Use Default Settings] から [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。

図 6-22 コンテンツ フィルタの選択解除  
Mail Policies: Content Filters

Content Filtering for Policy: Engineering			
Enable Content Filtering for this Policy:			<input checked="" type="radio"/> Yes <input type="radio"/> Use Default Settings <input type="radio"/> No
Content Filters			
Order	Filter Name	Description	Enable
1	scan_for_confidential	scan all incoming email for the string "confidential"	<input checked="" type="checkbox"/>
2	no_mp3s	strip all mp3 attachments	<input type="checkbox"/>
3	ex_employee	bounce messages intended for Doug	<input checked="" type="checkbox"/>
Cancel			Submit

- ステップ 4** [Submit] をクリックします。
- [Incoming Mail Policies] ページが表示され、テーブルが更新され、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が示されます。

図 6-23 コンテンツ フィルタが更新された [Incoming Mail Policies]

Policies						
Add Policy...						
Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	Sales_Group	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	(use default)	(use default)	(use default)	🗑️
2	Engineering	(use default)	(use default)	scan_for_confidential ex_employee	Enabled	🗑️
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	scan_for_confidential no_mp3s ex_employee	Enabled	

**ステップ 5** 変更を確定します。

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一致します）。
- 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。

図 6-24 任意またはすべての条件の選択

Add Filter	
Name:	<input type="text"/>
Currently used by policies:	
Description:	<input type="text"/>
Order:	5 <input type="button" value="v"/>
Apply filter:	<input checked="" type="radio"/> If one or more conditions match <input type="radio"/> Only if ALL conditions match

- 「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、着信または発信コンテンツ フィルタの「マスター 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。
  - [Incoming Content Filters] または [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。
  - [Incoming Mail Policies] または [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 [Quarantine] アクションは、作成する検疫エリアの保持設定に役に立ちます（詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Quarantines」の章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、検疫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）、システム検疫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 クエリー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 サーバをクエリー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、[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ることで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 6-25 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 フィルタの要件ページで、[Description]、[Rules] および [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。
  - [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）。
  - [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。
  - [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。

図 6-26 コンテンツ フィルタの [Description]、[Rules] および [Policy] を切り替えるリンクの使用

### Incoming Content Filters

Filters				
Add Filter...				
Order	Filter Name	Description   Rules   Policies	Duplicate	Delete
1	scan_for_confidential	scan_for_confidential: if (body-contains("confidential")) { quarantine ("Policy"); bcc ("hr@example.com", "[message matched confidential filter]"); }		
2	no_mp3s	no_mp3s: if (true) { drop-attachments-by-filetype("mp3", "mp3 deleted"); }		
3	ex_employee	ex_employee: if (rcpt-to == "^doug@") { notify-copy ("{\$EnvelopeSender", "message bounced for ex-employee of example.com"); bounce(); }		
4	drop_large_attachments	drop_large_attachments: if (true) { drop-attachments-by-size(5242880, "This attachment was too big!"); }		