

CHAPTER 8

アンチスパム

IronPort アプライアンスは、独自の階層化された方法により、電子メール ゲートウェイでスパムを阻止します。スパム制御の最初の階層である評価フィルタリング（第 7 章「評価フィルタリング」で前述）を使用すると、送信者の信頼性（IronPort SenderBase™ 評価サービスにより決定）に基づいて電子メールの送信者を分類し、ご使用の電子メール インフラストラクチャへのアクセスを制限できます。2 番目の防衛階層であるスキャンでは、IronPort Anti-Spam テクノロジーと IronPort Intelligent Multi-Scan テクノロジーが使用されています。評価フィルタリングとアンチスパム スキャンを組み合わせることにより、現在使用可能なものの中では最高水準の効率と性能を持つアンチスパム ソリューションが実現されています。

IronPort アプライアンスを使用すると、既知または信頼性の高い送信者、つまりお客様やパートナーなどからのメッセージに対して、アンチスパム スキャンを一切実施しないでエンドユーザーに直接配信するポリシーを非常に簡単に作成できます。未知または信頼性の低い送信者からのメッセージは、アンチスパム スキャンの対象にできます。また、各送信者から受け入れるメッセージの数をスロットリングすることもできます。信頼性の最も低い電子メール送信者に対しては、設定に基づいて接続を拒否したり、その送信者からのメッセージをドロップしたりできます。

IronPort アプライアンスの提供する独自の二層スパム対策により、高性能で今までにない柔軟性を備えた、企業の電子メール ゲートウェイ管理および保護が可能になります。

この章は、次の内容で構成されています。

- 「アンチスパムの概要」 (P.8-260)
- 「IronPort Anti-Spam フィルタリング」 (P.8-264)
- 「IronPort Intelligent Multi-Scan フィルタリング」 (P.8-271)

- 「アンチスパム ルールのアップデートの設定」 (P.8-275)
- 「アンチスパムの受信者別ポリシーの設定」 (P.8-276)
- 「着信リレー」 (P.8-288)

アンチスパムの概要

IronPort アプライアンスでは、IronPort Anti-Spam エンジンと IronPort Intelligent Multi-Scan の 2 つのアンチスパム ソリューションを提供しています。IronPort アプライアンスでこれらのソリューションのライセンスを許諾し、イネーブルにすることはできますが、同じポリシーに対して両方をイネーブルにはできません。電子メール セキュリティ マネージャを使用すると、異なるユーザのグループに対して異なるアンチスパム ソリューションをすばやく簡単に指定できます。

アンチスパム スキャンのイネーブル化

System Setup Wizard (または CLI の `systemsetup` コマンド) を使用すると、IronPort Intelligent Multi-Scan と IronPort Anti-Spam エンジンのいずれかをイネーブルにするオプションが示されます。システム セットアップの間に両方をイネーブルにはできませんが、システム セットアップの完了後に [Security Services] メニューを使用して、選択しなかったアンチスパム ソリューションをイネーブルにすることはできます。システム セットアップでは、陽性および陽性と疑わしいスパムに対処する IronPort スпам検査を必要に応じてイネーブルにすることができます。

IronPort スпам検査エンジンを初めてイネーブルにするときは (システム セットアップ時または後刻)、ライセンス契約書を読んで承諾してください。

図 8-1 アンチスパム エンジン : システム セットアップ時に選択

Anti-Spam	
SenderBase Reputation Filtering	<p>SenderBase Reputation Filtering provides a "first line of defense" against incoming spam by restricting access to your email infrastructure based on senders' trustworthiness as determined by their SenderBase Reputation Score (SBRs). More about SBRs...</p> <p><input checked="" type="checkbox"/> Enable SenderBase Reputation Filtering</p>
Anti-Spam Scanning	<p>Select the anti-spam engine to use for the default incoming mail policy:</p> <p><input type="radio"/> None</p> <p><input checked="" type="radio"/> IronPort Anti-Spam</p> <p><input checked="" type="checkbox"/> Enable IronPort Spam Quarantine. This setting will quarantine positive and suspect spam.</p>



(注)

アンチスパム スキャンの適用方法および適用条件については、「[電子メール パイプラインとセキュリティ サービス](#)」(P.4-99) を参照してください。

システムのセットアップが終了すれば、[Mail Policies] > [Incoming Mail Policies] ページから着信メール ポリシー用のアンチスパム スキャン ソリューションを設定できます (発信メール ポリシーでは、通常は、アンチスパム スキャンをディセーブルにします)。単一のポリシーについてアンチスパム スキャンをディセーブルにすることもできます。

この例では、デフォルト メール ポリシーおよび「Partners」ポリシーで IronPort Anti-Spam スキャン エンジンを使用して、陽性および陽性と疑わしいスパムを検査しています。

図 8-2 メール ポリシー : 受信者ごとのアンチスパム エンジン
Incoming Mail Policies

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

Key: Default Custom Disabled

IronPort Intelligent Multi-Scan を使用して不要なマーケティング メッセージをスキャンするように Partners ポリシーを変更するには、[Partners] 行に対応する [Anti-Spam] 列のエントリ (「use default」) をクリックします。

スキャン エンジンとして IronPort Intelligent Multi-Scan を選択し、[Yes] を選択して不要なマーケティング メッセージの検出をイネーブルにします。不要なマーケティング メッセージの検出には、デフォルト設定値を使用します。

図 8-3 に、IronPort Intelligent Multi-Scan と不要なマーケティング メッセージの検出がイネーブルにされたポリシーを示します。

図 8-3 メール ポリシー : IronPort Intelligent Multi-Scan のイネーブル化

Anti-Spam Settings	
Policy:	Test
Enable Anti-Spam Scanning for This Policy:	<input type="radio"/> Use Settings from Default Policy (IronPort Anti-Spam) <input type="radio"/> Use IronPort Anti-Spam service <input checked="" type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i> <input type="radio"/> Disabled
Positively-Identified Spam Settings	
Apply This Action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="button" value="v"/> [SPAM] <input type="text"/>
<input type="button" value="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:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="button" value="v"/> [SUSPECTED SPAM] <input type="text"/>
<input type="button" value="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 <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="button" value="v"/> [MARKETING] <input type="text"/>
<input type="button" value="Advanced"/> Optional settings for custom header and message delivery.	

変更の送信と確定後のメール ポリシーは次のようになります。

図 8-4 メール ポリシー : Intelligent Multi-Scan がイネーブルにされたポリシー

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
1	Partners	IronPort Intelligent Multi-Scan Positive: Deliver Suspected: Deliver Marketing Messages: Deliver	(use default)	(use default)	(use default)	<input type="button" value="trash"/>
	Default Policy	IronPort Anti-Spam Positive: Deliver Suspected: Deliver Marketing Messages: Disabled	Not Available	Disabled	Not Available	

Key:

アンチスパム スキャン エンジンの設定値

各アンチスパム ソリューションには、一連の設定値が関連付けられています。これらの設定値は、対応するエンジンだけに適用される設定で、[Security Services] メニューの [IronPort Anti-Spam] ページと [IronPort Intelligent Multi-Scan] ページおよび着信と発信のメール ポリシーのアンチスパム設定値 ページで使用可能です。スキャン ソリューション固有の設定値については、対応する項で説明します。[IronPort Anti-Spam] ページおよび [IronPort Intelligent Multi-Scan] ページには、最新のアップデート日時を持つアンチスパム ルールのリストも表示されます。

グローバル アンチスパム設定値を設定するときの詳細については、次の資料を参照してください。

- 「[IronPort Anti-Spam のイネーブル化とグローバル設定値の設定](#)」 (P.8-267) および
- 「[IronPort Intelligent Multi-Scan のイネーブル化とグローバル設定値の設定](#)」 (P.8-272)

受信者ごとの設定を原則とするアンチスパム スキャン設定の詳細については、「[アンチスパムの受信者別ポリシーの設定](#)」 (P.8-276) を参照してください。

アンチスパム スキャンと IronPort アプライアンスによって生成されるメッセージ

IronPort では、IronPort アプライアンスから電子メール アラート、スケジュール済みレポート、およびその他の自動化されたメッセージを受信する受信者の場合は、アンチスパム スキャンをバイパスする着信メール ポリシーに入れるよう推奨しています。これらのメッセージは、企業のメール ストリームでは通常見つかることのない、スパム発信元と関連性のある URL やその他の情報を含むため、これらのメッセージには、スパムとマークされることがあります。または、IronPort アプライアンスのためにメールの送信元の IP アドレスをホスト アクセステーブルの「WHITELIST」ポリシーに追加することもできます（「[送信者グループへの送信者の追加](#)」 (P.5-153) を参照）。詳細については、認可された IronPort アプライアンス サポート センターにお問い合わせください。

IronPort Anti-Spam フィルタリング

IronPort アプライアンスには、統合された IronPort Anti-Spam スキャン エンジン用の 30 日間のライセンスが含まれています。

IronPort Anti-Spam および CASE の概要

IronPort Anti-Spam フィルタリングは、Context Adaptive Scanning Engine (CASE)™ に基づいており、次の目的のために電子メールと Web 評価情報を組み合わせる、1 層めのアンチスパム スキャン エンジンです。

- 最大限多様な電子メール脅威の排除：スパム、フィッシング、ゾンビベースの攻撃、および他の「混合された」脅威を検出します。
- 最大限の精度の実現：SenderBase 評価サービスからの電子メールと Web 評価に基づくアンチスパム ルール。
- 扱いやすさ：ハードウェア コストおよび管理コストの低減を背景とします。
- 業界トップ クラスの性能の実現：CASE では、ダイナミックな初期終了基準およびオフボックス ネットワーク見積もりを使用して、きわめて優れた性能を実現できます。
- インターナショナル ユーザのニーズに対応：IronPort Anti-Spam は、世界的に業界トップ クラスの性能を発揮するように調整されています。

最大限多様な脅威防止

CASE では、コンテンツ分析、電子メール評価、および Web 評価を組み合わせ、最大限多様な脅威防止要因を収集します。

IronPort Anti-Spam は、できるだけ多様な電子メール脅威を徹底的に検出するように設計されています。IronPort Anti-Spam では、スパム、フィッシング、ゾンビ攻撃などの既知のあらゆる脅威に対応するだけでなく、「419」詐欺など検出が難しく、少量で、短期間の電子メール脅威にも対応します。さらに、IronPort Anti-Spam では、ダウンロード URL または実行ファイルを介して不正なコンテンツを配布するスパム攻撃など、新しい脅威や混合された脅威を識別します。

IronPort Anti-Spam では、これらの脅威を識別するために、業界随一の網羅性を持つ脅威検出方式を使用し、メッセージのコンテキスト全体、つまりメッセージの内容、メッセージの構築方式、送信者の評価、メッセージでアドバタイズされている Web サイトの評価などを調べます。IronPort Anti-Spam だけが、電子

メールと Web の評価データを組み合わせ、世界有数の規模を誇る電子メールおよび Web トラフィックのモニタリング ネットワークである SenderBase の検出力を最大限活用して、新しい攻撃が開始され次第その攻撃を検出します。



(注) ローカル MX/MTA からのメールを受信するよう IronPort アプライアンスを設定している場合は、送信者の IP アドレスをマスクする可能性のあるアップストリーム ホストを指定する必要があります。詳細については、「[着信リレー](#)」(P.8-288) を参照してください。

最小限の false positive 率

IronPort Anti-Spam および IronPort ウイルス感染フィルタでは、特許出願中の Context Adaptive Scanning Engine (CASE) TM を利用しています。CASE では、4 つの次元にまたがる 100,000 個以上のメッセージ属性を分析することにより、めざましい精度と性能の向上を実現しています。

- ステップ 1 電子メール評価：このメッセージの送信者は誰か。
- ステップ 2 メッセージの内容：このメッセージに含まれている内容は何か。
- ステップ 3 メッセージ構造：このメッセージはどのように構築されているか。
- ステップ 4 Web 評価：遷移先はどこか。

CASE では、多次元な関係を分析することにより、優れた精度を維持しながら、多様な脅威を検出できます。たとえば、正規金融機関から送信されたと断言する内容を持ちながら、消費者向けのブロードバンド ネットワークに属している IP アドレスから送信されたメッセージや、ゾンビ PC によってホストされている URL を含むメッセージは、疑わしいメッセージであると見なされます。これとは対照的に、肯定的な評価が与えられている製薬会社からのメッセージは、スパムとの関連性が強い単語を含んでいたとしても、スパムであるとタグ付けされません。

業界トップ水準の性能

CASE では、次の機能を組み合わせることにより、正確な判定が迅速に実行されます。

- 単一パスによる複数脅威のスキャン
- 動的な「初期終了」システム

システム性能は、IronPort 固有の「初期終了」システムを使用して最適化されます。IronPort では、ルールの精度と計算コストに基づいてルールの適用順序を決定する、独自のアルゴリズムを開発しました。コストが低い一方で正確性の高いルールから実行していき、判定が出た時点でそれ以降のルールは不要になります。この方式によってシステムのスループットが向上されるため、大企業のニーズを満たす製品が実現されます。反対に、高効率なエンジンは低コストハードウェアへの実装を可能にしているため、IronPort のセキュリティ サービスはローエンドのお客様にとって魅力的です。

- オフボックス ネットワーク見積もり

インターナショナル ユーザ

IronPort Anti-Spam は、業界トップクラスの性能をワールドワイドで発揮するように調整されています。ロケール固有でありコンテンツに依存する脅威検出技術に加え、リージョナルルールプロファイルを使用することによって、特定のリージョン向けにアンチスパム スキャンを最適化できます。アンチスパム エンジンには、リージョナルルールプロファイルが含まれています。リージョナルルールプロファイルでは、リージョナルベースでスパムをターゲットにします。たとえば、中国および台湾で受信するスパムでは、繁体字および簡体字の割合が高くなります。中国語のリージョナルルールは、このタイプのスパムに合わせて最適化されています。主に中国本土、台湾、および香港向けのメールを受信するのであれば、中国語のリージョナルルールプロファイルを使用することを、強く推奨します。リージョナルルールプロファイルは、[Security Services] > [IronPort Anti-Spam] からイネーブルにできます。



(注) リージョナルルールプロファイルでは特定のリージョンに合わせてアンチスパム エンジンが最適化されるため、他のタイプのスパムについては検出率の低下を招くおそれがあります。したがって、指定したリージョンから大量の電子メールを受信する場合に限り、この機能をイネーブルにすることを推奨します。

IronPort Anti-Spam では、南北アメリカ大陸、ヨーロッパ、およびアジアに散在している、125,000 を超える ISP、大学、および企業から提供された、地球規模において代表的な電子メールと Web のコンテンツ不可知データを活用しています。サンパウロ、北京、およびロンドンに中枢機能を置く Threat Operations Center が世界的活動のために設置されています。さらに、中国語、日本語、韓国語、ポルトガル語、およびスペイン語を含む 32 の言語からの専門家たちが加わっています。

IronPort Anti-Spam のイネーブル化とグローバル設定値の設定

概要

IronPort Anti-Spam のイネーブル化とグローバル設定値の変更には、[Security Services] > [IronPort Anti-Spam] ページと [Security Services] > [Service Updates] ページ (GUI) または `antisppamconfig` コマンドと `updateconfig` コマンド (CLI) を使用します。次のグローバル設定値が設定されます。

- アプライアンスの IronPort Anti-Spam をグローバルでイネーブルにします。
- IronPort Anti-Spam でスキャンするメッセージの最大サイズを設定します。
- メッセージをスキャンするときにタイムアウトを待機する時間の長さを入力します。

大部分のユーザでは、スキャンする最大メッセージサイズもタイムアウト値も変更する必要がありません。ただし、最大メッセージサイズ設定を小さくすると、アプライアンスのスループットを最適化できます。

- IronPort Anti-Spam ルールのアップデートを取得するためのプロキシサーバを定義し、必要に応じてイネーブルにします ([Security Services] > [Service Updates])。ルールのアップデートを取得するためのプロキシサーバを定義する場合は、必要に応じて、プロキシサーバに接続するための認証済みユーザ名、パスワード、および特定のポートを設定できます。
- IronPort Anti-Spam ルールのアップデートを受信するダウンロードサーバを定義し、必要に応じてイネーブルにします ([Security Services] > [Service Updates])。
- IronPort Anti-Spam ルールの自動アップデートの受信をイネーブルまたはディセーブルにし、アップデート間隔も指定します。



(注) プロキシサーバのセットアップは、[Security Services] > [Service Updates] ページから行うことができます。プロキシサーバの指定方法の詳細については、「[Service Updates] ページ」(P.15-487) を参照してください。これで、プロキシサーバがグローバルになったため、プロキシサーバを使用するように設定されているすべてのサービスで同じプロキシサーバが使用されます。



(注) GUI の System Setup Wizard (または CLI の `systemsetup` コマンド) で IronPort Anti-Spam をイネーブルにすることを選択した場合は、グローバル設定値のデフォルト値を使用し、デフォルト着信メール ポリシーに対してイネーブルになります。

評価キー

IronPort アプライアンスには、IronPort Anti-Spam ソフトウェアの 30 日間有効な評価キーが付属しています。このキーは、System Setup Wizard または [Security Services] > [IronPort Anti-Spam] ページ (GUI) か、`systemsetup` コマンドまたは `antispsamconfig` コマンド (CLI) で、ライセンス契約書を受諾して初めてイネーブルになります。デフォルトでは、ライセンス契約書に同意すると、デフォルト着信メール ポリシーに対して IronPort Anti-Spam がイネーブルになります。設定した管理者アドレス (「手順 2 : [System]」(P.3-54) を参照) に対して、IronPort Anti-Spam のライセンスの期限が 30 日後に切れることを通知するアラートの送信も行われます。アラートは、期限切れの 30、15、5、および 0 日前に送信されます。30 日間の評価期間後もこの機能をイネーブルにする場合の詳細については、IronPort の営業担当者にお問い合わせください。残りの評価期間は、[System Administration] > [Feature Keys] ページを表示するか、または `featurekey` コマンドを発行することによって確認できます (詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Common Administrative Tasks」にある機能キーの使用に関する項を参照してください)。

図 8-5 に、[Security Services] > [IronPort Anti-Spam] ページで設定するグローバル設定値を示します。

図 8-5 IronPort Anti-Spam のグローバル設定値 : 編集

IronPort Anti-Spam Global Settings	
IronPort Anti-Spam Scanning:	Enabled
Maximum Message Size to Scan:	131072 bytes
Timeout for Scanning Single Message:	1m
Regional Scanning:	Off

[Edit Global Settings...](#)

IronPort Anti-Spam をイネーブルにするには、次の手順を実行します。

- ステップ 1** System Setup Wizard で IronPort Anti-Spam をイネーブルにしなかった場合は、[Security Services] > [IronPort Anti-Spam] を選択します。


ステップ 2 [Enable] をクリックします。

ライセンス契約書ページが表示されます。



(注) ライセンス契約に合意しない場合、IronPort Anti-Spam はアプライアンスでイネーブルになりません。

ステップ 3 ページの下部までスクロールし、[Accept] をクリックしてライセンス契約に合意します。

 **8-6** とほぼ同じページが表示されます。

ステップ 4 [Edit Global Settings] をクリックします。

ステップ 5 [Enable IronPort Anti-Spam scanning] の横のボックスをオンにします。

このボックスをオンにすると、アプライアンスの機能がグローバルにイネーブルになります。ただし、メール ポリシーの受信者ごとの設定値をイネーブルにする必要は、引き続きあります。詳細については、「[アンチスパムの受信者別ポリシーの設定](#)」(P.8-276) を参照してください。

ステップ 6 IronPort Anti-Spam でスキャンする最大メッセージサイズの値を選択します。

デフォルト値は 128 Kb です。このサイズより大きいメッセージは、IronPort Anti-Spam によってスキャンされず、X-IronPort-Anti-Spam-Filtered: true というヘッダーはメッセージに追加されません。

ステップ 7 メッセージをスキャンするときにタイムアウトを待機する秒数を入力します。

秒数を指定する場合は、1 ~ 120 の整数を入力します。デフォルト値は 60 秒です。

ステップ 8 リージョナル スキャンをイネーブルまたはディセーブルにします。リージョナル スキャンでは、特定のリージョン用に IronPort Anti-Spam スキャンが最適化されます。この機能では特定のリージョンに合わせてアンチスパム エンジンが最適化されるため、他のタイプのスパムについては検出率の低下を招くおそれがあります。したがって、指定したリージョンから大量の電子メールを受信する場合に限り、この機能をイネーブルにすることを推奨します。リージョナル スキャンの詳細については、「[インターナショナル ユーザ](#)」(P.8-266) を参照してください。

ステップ 9 変更を送信して確定します。

[Security Services] > [IronPort Anti-Spam] ページがリフレッシュされて、前の手順で選択した値が表示されます。

図 8-6 IronPort Anti-Spam のグローバル設定値
IronPort Anti-Spam

IronPort Anti-Spam Overview	
IronPort Anti-Spam Scanning:	Enabled
Maximum Message Size to Scan:	131072 bytes
Timeout for Scanning Single Message:	60 seconds
Regional Scanning:	Off
Edit Global Settings...	

Rule Updates (Last download attempt made on: 03 Apr 2007 21:06 (GMT))		
Rule Type	Last Update	Current Version
CASE Core Files	03 Apr 2007 21:06 (GMT)	1.1.7-008
Structural Rules	03 Apr 2007 21:06 (GMT)	1.1.7-005-20070402_170501
Content Rules	03 Apr 2007 21:06 (GMT)	20070403_205114
Content Rules Update	03 Apr 2007 21:06 (GMT)	20070403_210501
CASE Utilities	03 Apr 2007 21:01 (GMT)	1.1.7-008
Web Reputation DB	03 Apr 2007 21:06 (GMT)	20070402_201000
Web Reputation Rules	03 Apr 2007 21:06 (GMT)	20070402_201000-20070403_210000
Update Now		

その他の手順

IronPort Anti-Spam をイネーブルにすると、SenderBase 評価スコアに基づいて接続を拒否していない場合であっても、SenderBase 評価サービスのスコアリングがイネーブルになります。SBRs のイネーブル化の詳細については、「[SenderBase 評価フィルタの実装](#)」(P.7-250) を参照してください。

IronPort Intelligent Multi-Scan フィルタリング

IronPort Intelligent Multi-Scan では、IronPort Anti-Spam などの複数のアンチスパム スキャン エンジンを組み込むことにより、インテリジェントな多層アンチスパム ソリューションを実現しています。この方式により、false positive 率を上昇させることなく、判定の精度が向上されて、検出されるスパムの量が増加します。

IronPort Intelligent Multi-Scan によってメッセージを処理する場合は、まず、サードパーティ製アンチスパム エンジンを使用してスキャンされます。次に、メッセージおよびサードパーティ製エンジンによる判定が IronPort Anti-Spam に渡されて、最終判定が下されます。IronPort Anti-Spam 自体によるスキャンの実行後に統合されたマルチスキャン評点が AsyncOS に返されます。サードパーティ製スキャン エンジンと IronPort Anti-Spam の長所を組み合わせることによって、IronPort Anti-Spam の持つ低い false positive 率を維持しながら、検出するスパムの数が増えます。

IronPort Intelligent Multi-Scan で使用されるスキャン エンジンの順序は設定できません。IronPort Anti-Spam は、常に最後にメッセージをスキャンするエンジンであり、サードパーティ製エンジンによってスパムであると判定されたメッセージを IronPort Intelligent Multi-Scan がスキップすることはありません。

IronPort Intelligent Multi-Scan を使用すると、システムのスループットが低下する場合があります。詳細については、IronPort サポート担当者にお問い合わせください。

この機能は、C100 アプライアンス以外のすべての C-Series アプライアンスおよび X-Series アプライアンスでサポートされています。



(注)

Intelligent Multi-Scan 機能キーによって、アプライアンスで IronPort Anti-Spam もイネーブルになります。その結果、メール ポリシーで IronPort Intelligent MultiScan または IronPort Anti-Spam のいずれかをイネーブルにできるようになります。

IronPort Intelligent Multi-Scan のイネーブル化とグローバル設定値の設定

概要

IronPort Intelligent Multi-Scan のイネーブル化とグローバル設定値の変更には、[Security Services] > [IronPort Intelligent Multi-Scan] ページと [Security Services] > [Service Updates] ページ (GUI) または `antisпамconfig` コマンドと `updateconfig` コマンド (CLI) を使用します。次のグローバル設定値が設定されます。

- アプライアンスでグローバルに IronPort Intelligent Multi-Scan をイネーブルにします。
- IronPort Intelligent Multi-Scan でスキャンするメッセージの最大サイズを設定します。
- メッセージをスキャンするときにタイムアウトを待機する時間の長さを入力します。

大部分のユーザでは、スキャンする最大メッセージサイズもタイムアウト値も変更する必要がありません。ただし、最大メッセージサイズ設定を小さくすると、アプライアンスのスループットを最適化できます。

- IronPort Intelligent Multi-Scan ルールのアップデートを取得するためのプロキシサーバを定義し、必要に応じてイネーブルにします ([Security Services] > [Service Updates])。ルールのアップデートを取得するためのプロキシサーバを定義する場合は、必要に応じて、プロキシサーバに接続するための認証済みユーザ名、パスワード、および特定のポートを設定できます。
- IronPort Intelligent Multi-Scan ルールのアップデートを受信するダウンロードサーバを定義し、必要に応じてイネーブルにします ([Security Services] > [Service Updates])。
- IronPort Intelligent Multi-Scan ルールの自動アップデートの受信をイネーブルまたはディセーブルにし、アップデート間隔も指定します。



(注) プロキシ サーバのセットアップは、[Security Services] > [Service Updates] ページから行うことができます。プロキシ サーバの指定方法の詳細については、「[Service Updates] ページ」(P.15-487) を参照してください。これで、プロキシ サーバがグローバルになったため、プロキシ サーバを使用するように設定されているすべてのサービスで同じプロキシ サーバが使用されます。



(注) GUI の System Setup Wizard (または CLI の `systemsetup` コマンド) で IronPort Intelligent Multi-Scan をイネーブルにすることを選択した場合は、グローバル設定値のデフォルト値を使用し、デフォルト着信メール ポリシーに対してイネーブルになります。

図 8-7 に、[Security Services] > [IronPort Intelligent Multi-Scan] ページで設定するグローバル設定値を示します。

図 8-7 IronPort Intelligent Multi-Scan のグローバル設定値 : 編集

IronPort Intelligent Multi-Scan Overview	
IronPort Intelligent Multi-Scan:	Enabled
Maximum Message Size to Scan:	131072 bytes
Timeout for Scanning Single Message:	60 seconds
Edit Global Settings...	

IronPort Intelligent Multi-Scan をイネーブルにするには、次の手順を実行します。

ステップ 1 System Setup Wizard で IronPort Intelligent Multi-Scan をイネーブルにしなかった場合は、[Security Services] > [IronPort Intelligent Multi-Scan] を選択します。

ステップ 2 [Enable] をクリックします。

ライセンス契約書ページが表示されます。



(注) ライセンス契約書を受諾しなければ、IronPort Intelligent Multi-Scan は アプライアンスでイネーブルにされません。

ステップ 3 ページの下部までスクロールし、[Accept] をクリックしてライセンス契約に合意します。

図 8-8 とほぼ同じページが表示されます。

ステップ 4 [Edit Global Settings] をクリックします。

ステップ 5 [Enable IronPort Intelligent Multi-Scan] の横のボックスをオンにします。

このボックスをオンにすると、アプライアンスの機能がグローバルにイネーブルになります。ただし、メール ポリシーの受信者ごとの設定値をイネーブルにする必要は、引き続きあります。詳細については、「[アンチスパムの受信者別ポリシーの設定](#)」(P.8-276) を参照してください。

ステップ 6 IronPort Intelligent Multi-Scan でスキャンする最大メッセージサイズの値を選択します。

デフォルト値は 128 Kb です。このサイズより大きいメッセージは、IronPort Intelligent Multi-Scan によってスキャンされません。

ステップ 7 メッセージをスキャンするときにタイムアウトを待機する秒数を入力します。

秒数を指定する場合は、1 ~ 120 の整数を入力します。デフォルト値は 60 秒です。

ステップ 8 変更を送信して確定します。

[Security Services] > [IronPort Intelligent Multi-Scan] ページがリフレッシュされて、前の手順で選択した値が表示されます。

図 8-8 IronPort Intelligent Multi-Scan のグローバル設定値
IronPort Intelligent Multi-Scan

IronPort Intelligent Multi-Scan Overview		
IronPort Intelligent Multi-Scan:	Enabled	
Maximum Message Size to Scan:	131072 bytes	
Timeout for Scanning Single Message:	60 seconds	
Edit Global Settings...		

Rule Updates (Last download attempt made on: Never)		
Rule Type	Last Update	Current Version
CASE Core Files	Base Version	2.7.1-005
Structural Rules	Base Version	2.7.1-005-20090511_160603
CASE Utilities	Base Version	2.7.1-005
Web Reputation DB	Never Updated	20050725_000000
Web Reputation Rules	Never Updated	20050725_000000-20050725_000000
Update Now		

その他の手順

IronPort Intelligent Multi-Scan をイネーブルにすると、SenderBase 評価スコアに基づいて接続を拒否していない場合であっても、SenderBase 評価サービスのスコアリングがイネーブルになります。SBRs のイネーブル化の詳細については、「[SenderBase 評価フィルタの実装](#)」(P.7-250) を参照してください。

アンチスパム ルールのアップデートの設定

IronPort Anti-Spam および IronPort Intelligent Multi-Scan のルールは、デフォルトでは、IronPort のアップデート サーバから取得されます。アップデート用のローカル サーバ、アップデートの取得に使用するプロキシサーバ、ルールのアップデートを確認するかどうかおよび確認する頻度を指定できます。アンチスパム ソリューションのアップデートを設定するには、[Security Services] > [Service Updates] ページの [Edit Update Settings] をクリックします。

詳細については、「サービスのアップデート」(P.15-486) を参照してください。

IronPort Anti-Spam ルールのアップデートを取得するプロキシサーバのイネーブル化

IronPort アプライアンスは、IronPort のアップデート サーバに直接接続して、アンチスパム ルールのアップデートを受け取るように設定されます。この接続は、ポート 80 の HTTP によって確立され、コンテンツは暗号化されます。ファイアウォールでこのポートを開くことを避ける場合は、アップデートされたルールをアプライアンスで受け取ることができる、プロキシサーバおよび具体的なポートを定義できます。

プロキシサーバを使用する場合は、任意で認証およびポートを指定できます。

プロキシサーバが定義されている場合、IronPort Anti-Spam および IronPort Intelligent Multi-Scan では、そのプロキシサーバを自動的に使用します。他のすべてのサービス アップデート（ウイルス感染フィルタ、Sophos Anti-Virus など）についてプロキシサーバをディセーブルにしないで、アンチスパム ソリューションについてプロキシサーバをオフにする方法はありません。



(注)

プロキシサーバを定義すると、プロキシサーバを使用するように設定されているすべてのサービス アップデートで、そのプロキシサーバが自動的に使用されます。

プロキシサーバの定義の詳細については、「HTTP プロキシサーバの指定 (任意)」(P.15-493) を参照してください。

モニタリング ルールのアップデート

ライセンス契約を受諾すると、最新の IronPort Anti-Spam ルールおよび IronPort Intelligent Multi-Scan ルールのアップデートが [Security Services] メニュー（GUI）および `antispamstatus` コマンド（CLI）の対応するページにリストされます。



(注)

アップデートが実行されていないか、サーバが設定されていない場合は、「Never Updated」という文字列が表示されます。

図 8-9 [Security Services] > [IronPort Anti-Spam] ページの [Rules Updates] セクション：GUI

Rule Updates (Last download attempt made on: 12 Sep 2005 21:43 GMT)		
Rule Type	Last Update	Current Version
CASE Core Files	Never Updated	1.0.0-202
Anti-Spam Rules	Never Updated	1.0.0-203-BETA-20050908_200919
CASE Utilities	Never Updated	1.0.0-105
URL Database	12 Sep 2005 05:39 GMT	20050908_184000
URL Database Delta	12 Sep 2005 21:42 GMT	20050908_184000-20050912_144000

[Update Now](#)

アンチスパムの受信者別ポリシーの設定

IronPort Anti-Spam ソリューションおよび IronPort Intelligent Multi-Scan ソリューションでは、電子メールセキュリティ マネージャ機能を使用して設定するポリシー（コンフィギュレーション オプション）に基づいて、着信（および発信）メール用の電子メールを処理します。IronPort Anti-Spam および IronPort Intelligent Multi-Scan では、フィルタリング モジュールによってメッセージをスキャンすることにより分類します。この分類、言い換えれば判定が、後続の配信アクションのために返されます。判定結果として得られる可能性があるのは、スパムでない、不要なマーケティング電子メール、陽性と判定されたスパム、または陽性と疑わしいスパムの 4 つです。スパム陽性と判定されたメッセージ、スパム陽性と疑わしいメッセージ、または不要なマーケティング メッセージであると識別されたメッセージに対するアクションには、次のアクションが含まれます。

- 陽性または陽性と疑わしいスパムのしきい値の指定。

- 不要なマーケティング メッセージ、陽性と判定されたスパム、または陽性と疑わしいスパム メッセージに対する全般的なアクションの選択：配信、ドロップ、バウンス、または検疫。
- mbox 形式のログ ファイルへのメッセージのアーカイブ。スパムであると識別されたメッセージのアーカイブをイネーブルにするには、ログを作成する必要があります。「識別されたメッセージのアーカイブ」(P.8-280) を参照してください。
- スパムまたはマーケティングであると識別されたメッセージの件名ヘッダーの変更。
- 代替宛先メールホストへのメッセージの送信。
- メッセージに対するカスタム X-Header の追加。
- 代替エンベロープ受信者アドレスへのメッセージの送信（たとえば、スパムであると識別されたメッセージを後で調査するために、管理者のメールボックスにルーティングできます）。複数受信者メッセージの場合は、単一のコピーだけが代替受信者に送信されます。



(注)

これらのアクションは、相互に排他的ではありません。ユーザのグループのさまざまな処理ニーズに合わせて、さまざまな着信または発信ポリシーで、これらのアクションを数個またはすべてを、さまざまに組み合わせることができます。同じポリシーで、陽性と判定されたスパムと陽性と疑わしいスパムを別々に扱うことができます。たとえば、陽性と判定されたスパムであるメッセージをドロップする一方で、陽性と疑わしいスパム メッセージを検疫する必要がある場合があります。

IronPort Anti-Spam または IronPort Intelligent Multi-Scan のアクションは、電子メール セキュリティ マネージャ機能を使用して、[Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページ (GUI) または `policyconfig -> antispaam` コマンド (CLI) から、受信者単位を基本にイネーブルにします。アンチスパム ソリューションがグローバルでイネーブルになってから、作成したメール ポリシーごとに、これらのアクションを個別に設定します。異なるメール ポリシーに対して異なるアクションを設定できます。ポリシーごとにイネーブルにできるアンチスパム ソリューションは 1 つだけです。同じポリシーでは両方をイネーブルにできません。



(注) 発信メールのアンチスパム スキャンをイネーブルにするには、関連するホストアクセス テーブルのアンチスパム設定値、特にプライベート リスナーも確認する必要があります。詳細については、「[メール フロー ポリシー : アクセスルールとパラメータ](#)」(P.5-117) を参照してください。

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。

図 8-10 メール ポリシー : アンチスパム エンジン

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)	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

メール ポリシーのアンチスパム設定値の編集

メール ポリシーのアンチスパム設定値をユーザごとに編集する処理は、ポリシーが着信メール用であっても、発信メール用であっても、基本的に同じです。

個々のポリシー（デフォルト以外）には、[Use Default] 設定値という追加のフィールドがあります。このフィールドを選択すると、デフォルト メールポリシーのすべてのアンチスパム設定値がポリシーに導入されます。

詳細については、「[デフォルトポリシーの編集 : アンチスパム設定](#)」(P.6-221) も参照してください。

デフォルト ポリシーなどのメールポリシーのアンチスパム設定値を編集する手順は、次のとおりです。

- ステップ 1** 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 テーブルの任意の行にある、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 8-11 に示すようなアンチスパム設定値ページが表示されます。

デフォルト ポリシーの設定を編集するには、デフォルト行のリンクをクリックします。図 8-11 は、具体的なポリシー（デフォルト以外）の設定値を示します。この画面と図 6-6 (P.6-223) を比較してください。[Use Default] オプションが個々のポリシーに付加されている状態に注意してください。

ステップ 2 ポリシーで使用するアンチスパム ソリューションを選択します。

[Disabled] をクリックすると、メール ポリシーのアンチスパム スキャン全体をディセーブルにできます。

ステップ 3 陽性と判定されたスパム、陽性と疑わしいスパム、および不要なマーケティングメッセージの設定値を設定します。

図 8-11 に、編集直前のデフォルト メール ポリシーの IronPort Anti-Spam 設定値を示します。「陽性と判定されたスパムと陽性と疑わしいスパム」(P.8-283) および「識別されたメッセージの設定値を設定する際の注意事項」(P.8-279) を参照してください。

ステップ 4 変更を送信して確定します。

[Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページがリフレッシュされて、これまでの手順で選択した値が反映されません。

識別されたメッセージの設定値を設定する際の注意事項

陽性および陽性と疑わしいスパムのしきい値

陽性と判定されたスパムおよび陽性と疑わしいスパムのしきい値に対する値を入力します。スパムしきい値の詳細については、「陽性および陽性と疑わしいスパムのしきい値」(P.8-281) を参照してください。

適用するアクション

陽性と判定されたスパム、陽性と疑わしいスパム、または不要なマーケティングメッセージに対する全般的なアクションを配信、ドロップ、バウンス、または検疫から選択します。

識別されたメッセージのアーカイブ

識別されたメッセージを「アンチスパム アーカイブ」ログにアーカイブできます。この形式は、mbox 形式のログ ファイルです。詳細については、下の例および『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Logging」の章を参照してください。

件名ヘッダーの変更

特定のテキスト文字列を前または後に追加して、識別されたメッセージ上の件名ヘッダーのテキストを変更することにより、スパムおよび不要なマーケティングメッセージをユーザが識別およびソートしやすくなります。



(注)

[Modify message subject] フィールドでは、空白は無視されません。このフィールドに入力したテキストの後ろまたは前にスペース追加することで、オリジナルのメッセージ件名と、追加テキストを分けることができます（追加テキストをオリジナルの件名の前に追加する場合は追加テキストの前、オリジナルの件名の後ろに追加する場合は追加テキストの後ろにスペースを追加します）。たとえば、前に追加する場合は、末尾に空白をいくつか付けて [SPAM] というテキストを追加します。



(注)

[Add text to message] フィールドでは、US-ASCII 文字だけを使用できます。

識別されたメッセージの代替宛先ホストへの送信

識別されたメッセージを代替宛先メールホストに送信できます。

カスタム X-Header の追加

識別されたメッセージにカスタム X-Header を追加できます。

[Yes] をクリックし、ヘッダー名およびテキストを定義します。

エンベロープ受信者アドレスの変更

識別されたメッセージを代替エンベロープ受信者アドレスに送信できます。

[Yes] をクリックし、代替アドレスを定義します。

たとえば、スパムであると識別されたメッセージを後で調査するために、管理者のメールボックスにルーティングできます。複数受信者メッセージの場合は、単一のコピーだけが代替受信者に送信されます。

図 8-11 メールポリシー用 IronPort Anti-Spam 設定値
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:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="button" value="v"/> <input type="text" value="[[SPAM]]"/>
<input type="button" value="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:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="button" value="v"/> <input type="text" value="[[SUSPECTED SPAM]]"/>
<input type="button" value="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 <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="button" value="v"/> <input type="text" value="[[MARKETING]]"/>
<input type="button" value="Advanced"/>	Optional settings for custom header and message delivery.
Spam Thresholds	
<i>Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.</i>	
IronPort Anti-Spam:	<input checked="" type="radio"/> Use the Default Thresholds <input type="radio"/> Use Custom Settings:
	Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100)
	Suspected Spam: Score > <input type="text" value="50"/> (minimum 25, cannot exceed positive spam score)
<input type="button" value="Cancel"/>	<input type="button" value="Submit"/>

陽性および陽性と疑わしいスパムのしきい値

メッセージがスパムであるかどうかを評価するときに、IronPort Anti-Spam および IronPort Intelligent Multi-Scan では、メッセージの総合スパム評点に達するために何千ものルールを適用します。精度の高さを維持するために、この両方のアンチスパムソリューションでは、デフォルトで高いしきい値に設定されています。90 ~ 100 の評点が返されるメッセージは、陽性と判定されたスパムであると見なされます。陽性と判定されたスパムのしきい値は、75 (最も積極的) ~ 99 (最も保守的) で変更できます。アンチスパムソリューションの設定に組織のスパム許容度を反映できます。IronPort Anti-Spam および IronPort

Intelligent Multi-Scan の両方に、メールポリシー単位で適用できる、設定可能な陽性スパムおよび陽性と疑わしいスパムのしきい値が用意されています。これを利用して、スパムとの類似が見られる一方で、正規のメッセージと共通する特徴も持つグレイゾーンメッセージを示す、「陽性と疑わしいスパム」という任意のカテゴリを作成できます。

この新しいカテゴリのしきい値設定を変更して異なる積極度に変更することにより、陽性と疑わしいスパム範囲に設定した評点未満のすべてのメッセージを、正規のメッセージであると見なし、陽性と疑わしいしきい値を超えており、陽性しきい値未満のすべてのメッセージを、陽性と疑わしいスパムと見なして、適宜処理するように設定できます。陽性と疑わしいスパムに対して実行する個別のアクションを定義することもできます。たとえば、「陽性と判定された」スパムをドロップする一方で、「陽性と疑わしい」スパムを検疫することができます。

入力する数値が大きいほど、メッセージを陽性と疑わしいスパムであると判定するために使用される **IronPort Anti-Spam** ルールのしきい値が高くなります。低いしきい値をイネーブルにして、その結果「スパムの可能性あり」とマークされるメッセージの数を増やすには（**false positive** 率が高くなる可能性あり）、小さい値を入力します。反対に、確実にスパムメッセージだけをフィルタリング対象にするには、大きい数値を入力します（一部のスパムを見逃す可能性あり）。デフォルト値は **50** です。この 2 つのカテゴリを使用する一般的な設定については、「**陽性と判定されたスパムと陽性と疑わしいスパム**」(P.8-283) を参照してください。

陽性と疑わしいスパムのしきい値は、**IronPort Anti-Spam** のメールポリシーごとに設定されます。

陽性と判定されたスパムと陽性と疑わしいスパム

IronPort Anti-Spam および IronPort Intelligent Multi-Scan では、陽性と判定されたスパムと陽性と疑わしいスパムが区別されるため（「[陽性および陽性と疑わしいスパムのしきい値](#)」(P.8-281)）、次のいずれかの方法でシステムを設定することが一般的です。

表 8-1 陽性と判定されたスパムおよび陽性と疑わしいスパムの一般的な設定の例

スパム	方式 1 のアクション (Aggressive)	方式 2 のアクション (Conservative)
陽性判定	ドロップ	メッセージの件名に「[Positive Spam]」を追加して配信
陽性と疑わしい	メッセージの件名に「[Suspected Spam]」を追加して配信	メッセージの件名に「[Suspected Spam]」を追加して配信

1 番めの設定方式では、陽性と疑わしいスパム メッセージだけにタグを付け、陽性と判定されたメッセージはドロップされます。管理者およびエンドユーザは、着信メッセージの件名行を調べて、**false positive** でないかどうかを確認でき、管理者は必要に応じて、陽性と疑わしいスパムのしきい値を調整できます。

2 番めの設定方式では、陽性と判定されたスパムおよび陽性と疑わしいスパムは、件名を変更して配信されます。ユーザは、陽性と疑わしいスパムおよび陽性と判定されたスパムを削除できます。この方式は、1 番めの方式よりも保守的です。

電子メール セキュリティ マネージャ機能を使用する、受信者ごとを基本とした積極的なポリシーと保守的なポリシーの混合の詳細については、[表 6-6 \(P.6-233\)](#) を参照してください。

不要なマーケティング メッセージの検出

IronPort Anti-Spam および IronPort Intelligent Multi-Scan では、スパムと正規送信元からの不要なマーケティング メッセージを区別できます。マーケティング メッセージはスパムと見なされませんが、組織やエンドユーザによっては、マーケティング メッセージを受信しないことを希望する場合があります。スパム同様、不要なマーケティング メッセージを配信、ドロップ、検疫、またはバ

ウンスすることを選択できます。メッセージの件名にテキストを追加することによって、不要なマーケティングメッセージにタグを付け、マーケティングであることを識別することもできます。

IronPort Anti-Spam および Intelligent Multi-Scan によって追加されるヘッダー

メール ポリシーで IronPort Anti-Spam スキャンまたは Intelligent Multi-Scan がイネーブルにされている場合、そのポリシーを通過する各メッセージでは、次のヘッダーがメッセージに追加されます。

```
X-IronPort-Anti-Spam-Filtered: true
```

IronPort Anti-Spam または Intelligent Multi-Scan によってフィルタリングされた各メッセージについては、別のヘッダーも挿入されます。このヘッダーには、メッセージのスキャンに使用された CASE ルールとエンジンのバージョンを IronPort Support で識別できる情報が含まれています。

```
X-IronPort-Anti-Spam: result
```

IronPort Intelligent Multi-Scan では、サードパーティ製アンチスパム スキャンエンジンからのヘッダーも追加します。

また、電子メール セキュリティ マネージャ機能を使用すると、特定のポリシーに従って陽性と判定されたスパム、陽性と疑わしいスパム、または不要なマーケティング メールであると識別されたメッセージであるすべてのメッセージに対して、さらに追加するカスタム ヘッダーを定義することもできます ([「カスタム X-Header の追加」\(P.8-280\)](#) を参照)。

skip-spamcheck アクションを使用して、特定のメッセージの IronPort Anti-Spam スキャンをスキップさせるメッセージ フィルタも作成できます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」にある「Bypass Anti-Spam System Action」を参照してください。

誤って分類されたメッセージの IronPort Systems への報告

分類が誤っていると思われるメッセージを、分析用に IronPort に報告できます。各メッセージは、専門家チームによってレビューされ、製品の精度と有効性を向上させるために使用されます。各メッセージは、RFC 822 添付ファイルとして、次のアドレスに転送してください。

- spam@access.ironport.com : 見逃されたスパムの報告用
- ham@access.ironport.com : false positive の報告用

誤って分類されたメッセージの報告の詳細については、IronPort ナレッジベースを参照するか、IronPort サポート プロバイダーにお問い合わせください。

IronPort Anti-Spam のテスト

アプライアンスの IronPort Anti-Spam 設定をすばやくテストする手順は、次のとおりです。

ステップ 1 メール ポリシーに対して IronPort Anti-Spam をイネーブルにします (上記)。

ステップ 2 X-Advertisement: spam というヘッダーを含むテスト電子メールをそのメールポリシーに含まれているユーザに送信します。

テストを目的として、IronPort Anti-Spam では、X-Advertisement: spam という形式の X-Header を含むすべてのメッセージをスパムであると見なします。このヘッダーを付けて送信したテストメッセージには、IronPort Anti-Spam によってフラグが設定され、メールポリシーに対して設定したアクション (「アンチスパムの受信者別ポリシーの設定」 (P.8-276)) が実行されることを確認できます。trace コマンドを使用してこのヘッダーを組み込むか、Telnet プログラムを使用して SMTP コマンドをアプライアンスに送信することができます。詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Testing and Troubleshooting」の章および付録 A 「アプライアンスへのアクセス」を参照してください。



(注) アプライアンスの IronPort Anti-Spam の設定をテストする別の方法として、メッセージのヘッダーを調べて IronPort Anti-Spam によって追加された特定のヘッダーを確認する方法もあります。「IronPort Anti-Spam および Intelligent Multi-Scan によって追加されるヘッダー」 (P.8-284) を参照してください。

アンチスパムの性能の評価

IronPort では、インターネットと直接接続した本物のメール ストリームを使用して製品を評価することを強く推奨しています。これは、IronPort Anti-Spam と IronPort Intelligent Multi-Scan のルールは、活発なスパム攻撃を防ぐためにすぐに追加され、攻撃が終結するとすぐに期限切れになるためです。したがって、古いメッセージを使用してテストすると、テスト結果が不正確になります。

「本物」を使用する場合は、スパムと見なされるメッセージが正しく処理されるシステム設定になっているのであれば、X-Advertisement: spam ヘッダーを使用するテスト方法が最適です。trace コマンドを使用するか ([Debugging Mail Flow Using Test Messages: Trace, page -446](#) を参照)、次の例を参照してください。

評価時に陥りがちな落とし穴には、次のようなものがあります。

- 再送信されたか、転送されたメールまたはカット アンド ペーストされたスパム メッセージによる評価

適切なヘッダー、接続 IP、シグニチャなどを持たないメールを使用すると、評点が不正確になります。

- 「難易度の高いスパム」だけをテスト

SBRS、ブラックリスト、メッセージフィルタなどを使用して「難易度の低いスパム」を取り除くと、全体の検出率が低くなります。

- 別のアンチスパム ベンダーによって検出されたスパムの再送信
- 以前のメッセージのテスト

CASE では、現行の脅威に基づいて、ルールがすぐに追加および削除されます。以前のメッセージのコレクションを使用してテストすると、結果は大幅に不正確になります。

例 :

SMTP コマンドを使用して、x-advertisement: spam ヘッダーを含むテストメッセージを、アクセス権のあるアドレスに送信します。テストアドレス宛でのメッセージを受信するようにメール ポリシーが設定されていること

(「パブリック リスナー (RAT) 上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ」(P.5-177) を参照) および HAT で受け入れられるテスト接続であることを確認してください。

```
# telnet IP_address_of_IronPort_Appliance_with_IronPort_Anti-Spam
port

220 hostname ESMTF

helo example.com

250 hostname

mail from: <test@example.com>

250 sender <test@example.com> ok

rcpt to: <test@address>

250 recipient <test@address> ok

data

354 go ahead

Subject: Spam Message Test

X-Advertisement: spam

spam test

.

250 Message MID accepted

221 hostname

quit
```

次に、テスト アカウントのメールボックスを調べて、メール ポリシーに設定したアクションに基づいてテスト メッセージが正しく配信されたことを確認します。

次の例を参考にしてください。

- 件名行が変更されている。
- 追加のカスタム ヘッダーが追加されている。
- メッセージが代替アドレスに配信された。
- メッセージがドロップされた。

着信リレー

着信リレー機能は、ネットワークのエッジにある 1 つまたは複数の Mail Exchange/Transfer エージェント (MX または MTA)、フィルタリング サーバなどを介して IronPort アプライアンスにメールを送信している外部マシンの IP アドレスを、IronPort アプライアンスで取得するために有用です。このタイプの設定では、IronPort アプライアンスで外部マシンの IP アドレスを自動的に認識しません。代わりに、外部マシンではなくローカル MX/MTA (着信リレー) から発信されたメールであると認識されます。IronPort Anti-Spam および IronPort Intelligent Multi-Scan では、外部送信者の正確な IP アドレスを必要としているため、IronPort アプライアンスにとってこの情報の取得は不可欠です。

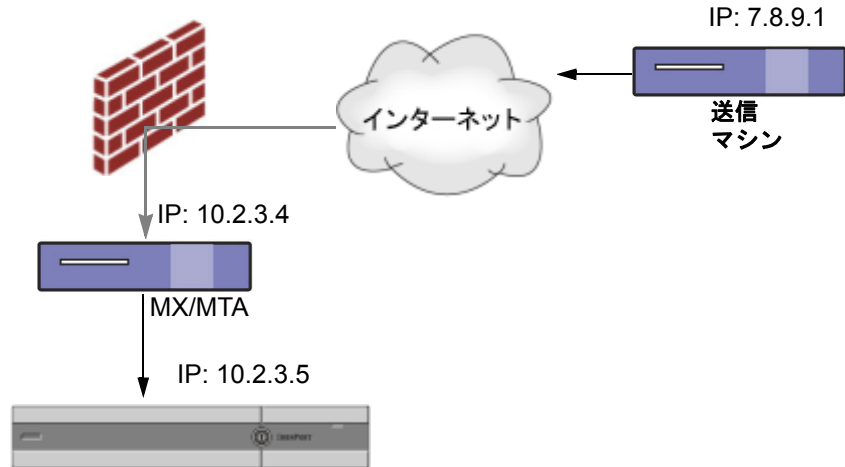


(注)

この機能は、IronPort アプライアンスにメールをリレーするローカル MX/MTA がある場合に限りイネーブルにしてください。

図 8-12 に、きわめて基本的な着信リレーの例を示します。ローカル MX/MTA によってメールが IronPort アプライアンスにリレーされているため、IP アドレス 7.8.9.1 からのメールは IP アドレス 10.2.3.4 からのように見えます。

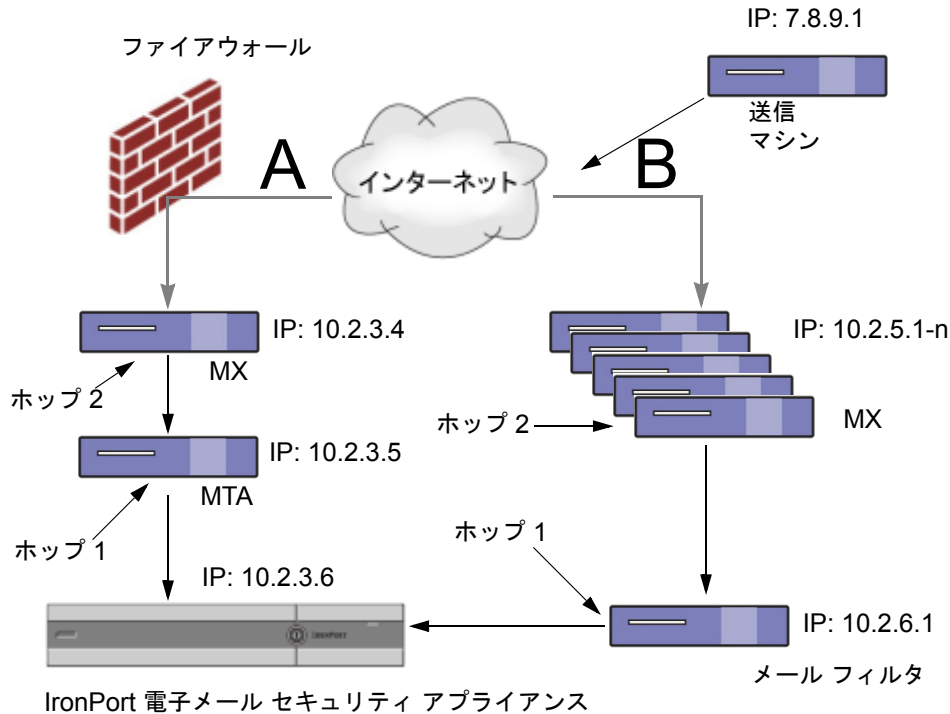
図 8-12 MX/MTA によるメール リレー：簡易
ファイアウォール



IronPort 電子メール セキュリティ アプライアンス

図 8-13 に別の 2 つの例を示します。この例は、少し複雑であり、ネットワーク内でのメールのリレー方法と、IronPort アプライアンスへの受け渡し前に実施できる、ネットワーク内の複数サーバにおけるメールの処理方法を示します。例 A では、7.8.9.1 からのメールがファイアウォールを通過し、MX および MTA で処理されてから、IronPort アプライアンスに配信されます。例 B では、7.8.9.1 からのメールがロード バランサまたは他のタイプのトラフィック シェーピング アプライアンスに送信され、一連の MX のいずれかに送信されてから、IronPort アプライアンスに配信されます。

図 8-13 MX/MTA によるメール リレー：拡張



着信リレー機能：概要

管理者は、インターネットからメールを直接受信する代わりに、ネットワークのエッジにある Mail Exchange (MX) または Mail Transfer Agent (MTA) の背後で IronPort アプライアンスを実行しなければならない場合があります。この設定を使用する場合、IronPort アプライアンスでは、残念ながらインターネットからメールを直接受信しないため、外部ネットワークからの直前の接続 IP アドレスが分かりません。受信メールは、代わりに、ローカル MX/MTA から受信されたことと示されます。接続 IP アドレスが既知であり、IronPort Intelligent Multi-Scan および IronPort Anti-Spam のスキャンで SenderBase 評価サービスを使用できることは、IronPort アプライアンスの正常な動作にとって不可欠です。

これは、着信リレーを設定することによって解決されます。着信リレーを設定するときは、IronPort アプライアンスに接続するすべての内部 MX/MTA の名前と IP アドレスおよび送信元 IP アドレスの格納に使用するヘッダーを指定します。ヘッダーを指定する方法は、カスタム ヘッダーと既存の Received ヘッダーの 2 通りあります。

着信リレーと電子メール セキュリティ モニタ

着信リレー機能を使用する場合、電子メール セキュリティ モニタによって準備されるデータには、外部 IP と MX/MTA の両方のデータが含まれています。たとえば、外部マシン (IP 7.8.9.1) から内部 MX/MTA (IP 10.2.3.4) を介して 5 通の電子メールが送信された場合、[Mail Flow Summary] には、IP 7.8.9.1 からの 5 個のメッセージに加えて、内部リレー MX/MTA (IP 10.2.3.5) からの 5 個のメッセージが表示されます。

着信リレーとフィルタ

着信リレー機能では、SenderBase 評価サービスに関連するさまざまなフィルタールール (reputation、no-reputation) に正しい SenderBase 評価スコアを提供します。

着信リレー、HAT、SBRS および送信者グループ

HAT ポリシー グループでは、着信リレーからの情報を現時点では使用していません。ことに注意してください。ただし、着信リレー機能では SenderBase 評価スコアを提供するため、メッセージフィルタおよび \$reputation 変数によって HAT ポリシー グループ機能をシミュレートできます。

着信リレーとレポート

着信リレーを使用している場合、電子メール セキュリティ モニタ レポートに示される SenderBase 評価スコアは正しくありません。送信者グループが正しく解決されない場合もあります。

IP アドレス

IronPort アプライアンスに接続するマシンの IP アドレス（着信リレー）を指定するときは、原則としてできるだけ個別に指定してください。つまり、IP アドレスは、標準 CIDR 形式または IP アドレスの範囲でも入力できます。たとえば、電子メールを受信する複数の MTA をネットワークのエッジに配置している場合に、すべての MTA を含む IP アドレスの範囲、たとえば 10.2.3.1/8 や 10.2.3.1-10 を入力する場合があります。

メッセージ ヘッダーと着信リレー

カスタム ヘッダー

カスタム ヘッダーを指定する場合に、この方法を使用します。これは推奨される方法です。元の送信者に接続するマシンでは、このカスタム ヘッダーを追加する必要があります。このヘッダーの値は、外部の送信マシンの IP アドレスになることが予期されます。次の例を参考にしてください。

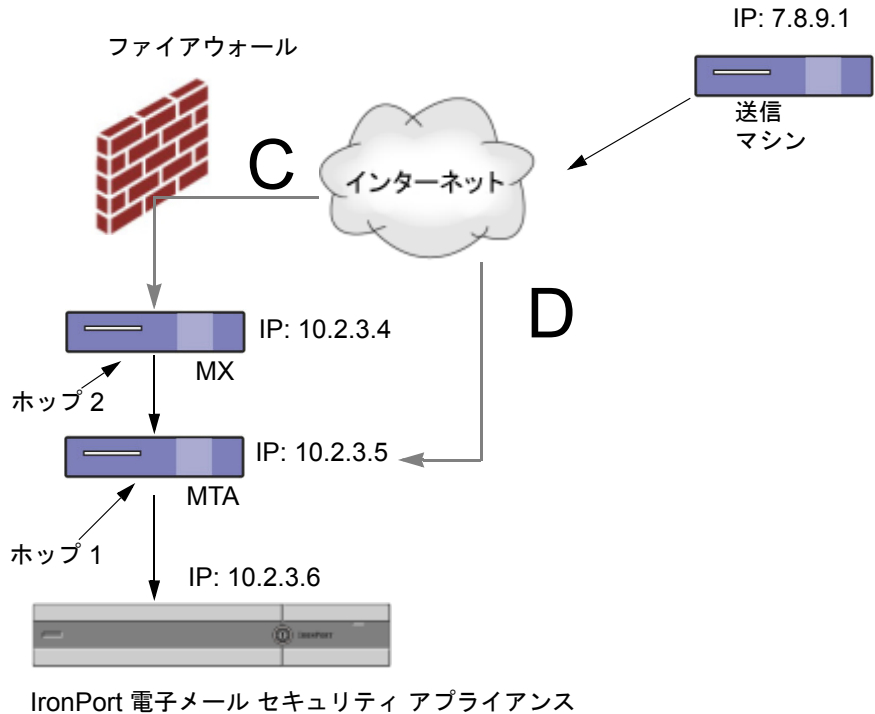
```
SenderIP: 7.8.9.1
```

```
X-CustomHeader: 7.8.9.1
```

ヘッダーを入力する場合に、末尾のコロンを入力する必要はありません。

ローカル MX/MTA で不定ホップ数のメールを受信する場合は、カスタム ヘッダーを挿入することが、着信リレー機能をイネーブルにする唯一の方法です。たとえば、[図 8-14](#) では、パス C とパス D の両方が IP アドレス 10.2.3.5 まで至る一方で、パス C は 2 ホップ、パス D は 1 ホップです。この状況では、ホップ数が異なる場合があるため、カスタム ヘッダーを使用して、着信リレーが正しく設定されるようにする必要があります。

図 8-14 MX/MTA によるメール リレー：不定ホップ数



Received ヘッダー

MX/MTA を設定する場合、送信 IP アドレスを含むカスタム ヘッダーの組み込みは選択肢になりません。着信リレー機能は、メッセージの「Received:」ヘッダーを調査することによって送信 IP アドレスの判別を試行するように設定できます。「Received:」ヘッダーを使用する方法は、ネットワーク ホップ数が常に一定である IP アドレスの場合に限り機能します。つまり、最初のホップにあるマシン (図 8-13 の 10.2.3.5) は、ネットワークのエッジからのホップ数が常に等しい必要があります。IronPort アプライアンスに接続しているマシンまでの着信メールのパスが異なる可能性がある場合 (したがって、図 8-14 で示したように、ホップ数が異なる場合) は、カスタム ヘッダーを使用する必要があります (「カスタム ヘッダー」 (P.8-292) を参照)。

解析対象文字または文字列および逆行して検索するネットワーク ホップ数 (または Received: ヘッダー数) を指定します。ホップは、基本的に、メッセージがマシン間で転送されることを指します (IronPort アプライアンスによる受信は

ホップとしてカウントされません。詳細については、「[使用されるヘッダーの特定](#)」(P.8-296)を参照してください)。AsyncOS は、指定されたホップ数に対応する Received: ヘッダー内の解析対象文字または文字列の最初のオカレンスに続く最初の IP アドレスを参照します。たとえば、2 ホップを指定した場合は、IronPort アプライアンスから逆行して 2 つめの Received: ヘッダーが解析されません。解析対象の文字が見つからないか、有効な IP アドレスが見つからない場合、IronPort アプライアンスでは、接続元マシンの実際の IP アドレスを使用します。

次のメールヘッダーの例で左角カッコ ([) と 2 ホップを指定した場合、外部マシンの IP アドレスは 7.8.9.1 です。ただし、右カッコ (]) および解析対象文字を指定した場合は、有効な IP アドレスが見つかりません。この場合、着信リレー機能はディセーブルであると見なされ、接続元マシンの IP (10.2.3.5) が使用されます。

図 8-13 の例における着信リレーは次のとおりです。

- パス A : 10.2.3.5 (Received ヘッダーを使用して 2 ホップ) および
- パス B : 10.2.6.1 (Received ヘッダーを使用して 2 ホップ)

表 8-2 に、図 8-13 同様、IronPort アプライアンスまで複数の移動ホップ数を持つメッセージの電子メールヘッダーの例を示します。この例は、受信者の受信箱に到着したメッセージで表示される、外部からのヘッダー (IronPort アプライアンスでは無視) を示します。指定するホップ数は 2 になります。表 8-3 に、外部ヘッダーを除いて、同じ電子メールメッセージのヘッダーを示します。

表 8-2 一連の Received: ヘッダー (パス A 例 1)

1	Microsoft Mail Internet Headers Version 2.0 Received: from smemail.rand.org ([10.2.2.7]) by smmail5.customerdoamin.org with Microsoft SMTPSVC(5.0.2195.6713); Received: from ironport.customerdomain.org ([10.2.3.6]) by smemail.customerdoamin.org with Microsoft SMTPSVC(5.0.2195.6713);
2	Received: from mta.customerdomain.org ([10.2.3.5]) by ironport.customerdomain.org with ESMTMP; 21 Sep 2005 13:46:07 -0700
3	Received: from mx.customerdomain.org (mx.customerdomain.org) [10.2.3.4]) by mta.customerdomain.org (8.12.11/8.12.11) with ESMTMP id j8LKkWu1008155 for <joefoo@customerdomain.org>

表 8-2 一連の Received: ヘッダー (パス A 例 1) (続き)

4	Received: from sending-machine.spamham.com (sending-machine.spamham.com [7.8.9.1]) by mx.customerdomain.org (Postfix) with ESMTF id 4F3DA15AC22 for <joefoo@customerdomain.org>
5	Received: from linux1.thespammer.com (HELO linux1.thespammer.com) ([10.1.1.89]) by sending-machine.spamham.com with ESMTF; Received: from exchangel.thespammer.com ([10.1.1.111]) by linux1.thespammer.com with Microsoft SMTPSVC(6.0.3790.1830); Subject: Would like a bigger paycheck? Date: Wed, 21 Sep 2005 13:46:07 -0700 From: "A.Sender" <asend@otherdomain.com> To: <joefoo@customerdomain.org>

表 8-2 についての注意事項は、次のとおりです。

-
- ステップ 1** IronPort アプライアンスでは、これらのヘッダーを無視します。
 - ステップ 2** IronPort アプライアンスがメッセージを受信します (ホップとしてカウントされない)。
 - ステップ 3** 最初のホップ (着信リレー)。
 - ステップ 4** 第 2 ホップ。これは、送信 MTA です。仮想 IP アドレスは 7.8.9.1 です。

ステップ 5 IronPort アプライアンスでは、これらの Microsoft Exchange ヘッダーを無視します。

表 8-3 一連の Received: ヘッダー (パス A 例 2)

1	Received: from mta.customerdomain.org ([10.2.3.5]) by ironport.customerdomain.org with ESMTTP; 21 Sep 2005 13:46:07 -0700
2	Received: from mx.customerdomain.org (mx.customerdomain.org) [10.2.3.4]) by mta.customerdomain.org (8.12.11/8.12.11) with ESMTTP id j8LkKwU1008155 for <joefoo@customerdomain.org>;
3	Received: from sending-machine.spamham.com (sending-machine.spamham.com [7.8.9.1]) by mx.customerdomain.org (Postfix) with ESMTTP id 4F3DA15AC22 for <joefoo@customerdomain.org>;

図 8-15 に、GUI の [Add Relay] ページで設定されたパス A の着信リレーを示します。

図 8-15 設定された着信リレー

Incoming Relay	
Name: ?	<input type="text" value="IncomingRelayOne"/>
IP Address: ?	<input type="text" value="10.2.3.5"/>
Header:	<input type="radio"/> Specify a custom header <input type="text" value=""/> <input checked="" type="radio"/> Parse the "Received" header
	Begin parsing after: ? <input type="text" value=""/> Hop: ? <input type="text" value="2"/>

使用されるヘッダーの特定

IronPort アプライアンスでは、メッセージが受信された時点で存在していたヘッダーだけを検査します。したがって、ローカルで追加される追加のヘッダー (Microsoft Exchange のヘッダーなど) や、IronPort アプライアンスがメッセージを受信するときに追加する追加のヘッダーは、処理されません。使用される

ヘッダーを特定する方法の 1 つは、logconfig CLI コマンドの logheaders サブコマンドを使用して、Received ヘッダーを AsyncOS ログに含めるよう設定することです。

```
mail3.example.com> logconfig
```

```
Currently configured logs:
```

```
[ ... list of configured logs ... ]
```

```
Choose the operation you want to perform:
```

- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
- CLUSTERSET - Set how logs are configured in a cluster.
- CLUSTERSHOW - Display how logs are configured in a cluster.

```
[> logheaders
```

```
Please enter the list of headers you wish to record in the log files.
```

```
Separate multiple headers with commas.
```

```
[> Received
```

着信リレー機能の設定 (GUI)

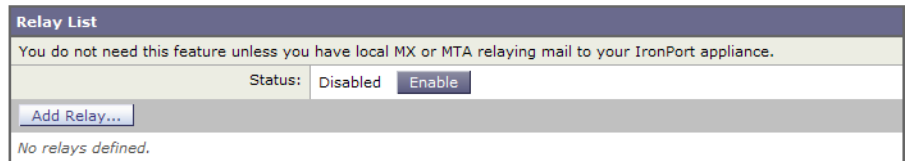
[Incoming Relays] ページは [Network] タブから使用可能です。

着信リレー機能のイネーブル化

着信リレー機能をイネーブルにした場合は、アプライアンスに対してグローバルでイネーブルになります (リレーはリスナー固有でない)。着信リレー機能をイネーブルにする手順は、次のとおりです。

- ステップ 1** [Network] タブの [Incoming Relays] リンクをクリックします。[Incoming Relays] ページが表示されます。

図 8-16 [Incoming Relays] ページ
Incoming Relays



- ステップ 2** [Enable] をクリックして、着信リレーをイネーブルにします (イネーブルにした着信リレー機能は、[Disable] をクリックすることによって、ディセーブルにできます)。
- ステップ 3** 変更を確定します。

着信リレーとメール ログ

次の例は、着信リレー情報を含む、一般的なログ エントリを示します。

```
Wed Aug 17 11:20:41 2005 Info: MID 58298 IncomingRelay(myrelay):
Header Received found, IP 192.168.230.120 being used
```

リレーの追加

リレーを追加する手順は、次のとおりです。

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

図 8-17 [Add Relay] ページ
Add Relay

Incoming Relay	
Name: ?	<input type="text"/>
IP Address: ?	<input type="text"/>
Header:	<input type="radio"/> Specify a custom header <input type="text"/>
	<input checked="" type="radio"/> Parse the "Received" header
	Begin parsing after: ? <input type="text" value="from"/>
	Hop: ? <input type="text" value="1"/>

Cancel Submit

- ステップ 2** リレーの名前を入力します。
- ステップ 3** リレーの IP アドレスを入力します。有効な IP アドレス エントリの詳細については、「[IP アドレス](#)」(P.8-292) を参照してください。
- ステップ 4** ヘッダー タイプ ([Custom] または [Received]) を選択します。カスタム ヘッダーの詳細については、「[カスタム ヘッダー](#)」(P.8-292) を参照してください。ヘッダーを入力する場合に、末尾のコロンを入力する必要はありません。
- カスタム ヘッダーの場合は、ヘッダー名を入力します。
 - **Received:** ヘッダーの場合は、IP アドレスの前に配置される文字または文字列を入力します。IP アドレスを調査するホップ数を入力します。詳細については、「[Received ヘッダー](#)」(P.8-293) を参照してください。
- ステップ 5** 変更を確定します。

リレーの編集

リレーを編集する手順は、次のとおりです。

- ステップ 1** [Incoming Relay] ページでリレーの名前をクリックします。[Edit Relay] ページが表示されます。
- ステップ 2** リレーに変更を加えます。
- ステップ 3** 変更を確定します。

リレーの削除

リレーを削除する手順は、次のとおりです。

- ステップ 1** 削除するリレーに対応する行のゴミ箱アイコンをクリックします。削除を確認するよう求められます。
- ステップ 2** [Delete] をクリックします。
- ステップ 3** 変更を確定します。

着信リレーとロギング

次のログの例で、送信者の SenderBase 評価スコアは、当初 1 行目に示されます。その後、着信リレーの処理が行われて、正しい SenderBase 評価スコアが 5 行目に示されます。

1	Fri Apr 28 17:07:29 2006 Info: ICID 210158 ACCEPT SG UNKNOWNLIST match nx.domain SBRS rfc1918
2	Fri Apr 28 17:07:29 2006 Info: Start MID 201434 ICID 210158
3	Fri Apr 28 17:07:29 2006 Info: MID 201434 ICID 210158 From: <joe@sender.com>
4	Fri Apr 28 17:07:29 2006 Info: MID 201434 ICID 210158 RID 0 To: <mary@example.com>
5	Fri Apr 28 17:07:29 2006 Info: MID 201434 IncomingRelay(senderdotcom): Header Received found, IP 192.192.108.1 being used, SBRS 6.8
6	Fri Apr 28 17:07:29 2006 Info: MID 201434 Message-ID '<7.0.1.0.2.20060428170643.0451be40@sender.com>'
7	Fri Apr 28 17:07:29 2006 Info: MID 201434 Subject 'That report...'
8	Fri Apr 28 17:07:29 2006 Info: MID 201434 ready 2367 bytes from <joe@sender.com>
9	Fri Apr 28 17:07:29 2006 Info: MID 201434 matched all recipients for per-recipient policy DEFAULT in the inbound table
10	Fri Apr 28 17:07:34 2006 Info: ICID 210158 close
11	Fri Apr 28 17:07:35 2006 Info: MID 201434 using engine: CASE spam negative

12	Fri Apr 28 17:07:35 2006 Info: MID 201434 antivirus negative
13	Fri Apr 28 17:07:35 2006 Info: MID 201434 queued for delivery

