CHAPTER 7

評価フィルタリング

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を使用すると、IronPort SenderBase™ 評価サービスにより決定される送信者の信頼性に基づいて、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 番めの防衛階層であるスキャン（次の章で説明します）では、IronPort Anti-Spam™ 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送り返したりできます。

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。

次章「アンチスパム」では、アンチスパム スキャン エンジンの詳細について説明します。

評価フィルタリング

SenderBase 評価サービスを使用すると、ユーザはリモート ホストの接続 IP アドレスに基づいて、正確かつ柔軟に陽性と疑わしいスパムを拒否またはスロットリングすることができます。SenderBase 評価サービスは、特定の送信元からのメッセージがスパムである可能性に基づいてスコアを返し、メール フロー モニタ機能で客観的データを示すことで、電子メール管理者が電子メールの送信元をより詳しく知ることができるようにします（『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」を参照）。SenderBase 評価サービスは、スタンドアロンのアンチスパム ソリューションとしても使用できます。IronPort Anti-Spam などの、コンテンツに基づいたアンチスパム システムの有効性を向上することを主な目的として設計されています。

SenderBase 評価サービスを使用することで、次のことが実行できます。

- スパムの低減

SenderBase 評価サービスを使用することで、企業は接続 IP アドレスに基づいて既知のスパムを特定し、スパムがゲートウェイに到達した時点で、組織がそのスパムをブロックできるようにします。これにより、使用されているアンチスパム スキャン エンジンまたはその他すべてのコンテンツに基づいたフィルタの有効性が高まります。

- スパム フラッドに対する保護

SoBig などのウイルスまたは「当て逃げ」スパム攻撃により、メッセージ量が予期せず急激に増加する場合があります。特定の送信者が大量の送信を開始した場合、SenderBase 評価サービスはグローバルなアフィリエイト ネットワークを介してこれを検出し、陰性スコアを割り当てることができます。IronPort アプライアンスは、このスコアを使用して、送信者に対して許可する 1 時間あたりの受信者数をただちに制限できます（「ウイルス感染フィルタ」（P.10-335）も参照してください）。

- スループットの向上

IronPort アプライアンスは、ただちに既知のスパムを拒否し、既知の良好なメッセージをコンテンツ フィルタを通過するようにルーティングすることで、システム負荷を低減し、メッセージのスループットを増加できます。

評価フィルタリング：IronPort SenderBase 評価サービス

IronPort SenderBase 評価サービス（http://www.senderbase.org から入手できます）は、送信者の身元に関する客観的なデータを提供することで、電子メール管理者による質の高い着信電子メール ストリーム管理の実現に役立つように設計されたサービスです。SenderBase 評価サービスは、電子メールの信用レポートに類似しています。企業は、SenderBase 評価サービスの提供するデータを使用して、正規の送信者とスパムの送信元を区別します。SenderBase 評価サービスは、IronPort アプライアンスの GUI に直接組み込まれており、ここで提供される客観的データを使用して、Unsolicited Commercial Email（UCE）を送信している IP アドレスの信頼性を識別したり、その IP アドレスをブロックしたり、またはビジネス パートナー、顧客、またはその他すべての重要な送信元からの正規着信電子メールの信頼性を確認したりできます。SenderBase 評価サービスは、電子メール メッセージの量をグローバルに表示して、電子メールの送信元の識別とグループ化を容易にする方法でデータを編成している点で独特です。

（注） IronPort アプライアンスが、ローカル MX/MTA から電子メールを受信するように設定されている場合は、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 ホストを識別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。

SenderBase 評価サービスには、次のような主要な要素があります。

- スプーフが不可能

電子メール送信者の信頼性は、電子メールの送信者の IP アドレスに基づいています。SMTP は、TCP/IP を使用した双方向のカンバセーションであるため、IP アドレスを「スプーフ」することはほぼ不可能です。提示される IP アドレスは、メッセージを送信しているサーバにより、実際に制御されているものである必要があります。

- 包括的

SenderBase 評価サービスは、慎重に選択された公開ブラックリストや、オープン プロキシ リストからのデータだけでなく、クレーム率およびメッセージ量の統計情報などの SenderBase Affiliate ネットワークからのグローバル データも使用して、特定の送信元からのメッセージがスパムである可能性を決定します。

- 設定可能

SenderBase 評価サービスは、単純にスパムであるかないか決定を返すブラックリストまたはホワイトリストなどの、その他の「身元に基づいた」アンチスパム手法とは異なり、送信元からのメッセージがスパムである可能性に基づいて、段階的な応答を返します。これにより、スパムをブロックするしきい値を独自に設定したり、SenderBase 評価スコアに基づいて送信者を自動的にさまざまなグループに割り当てたりできます。

SenderBase 評価スコア（SBRS）

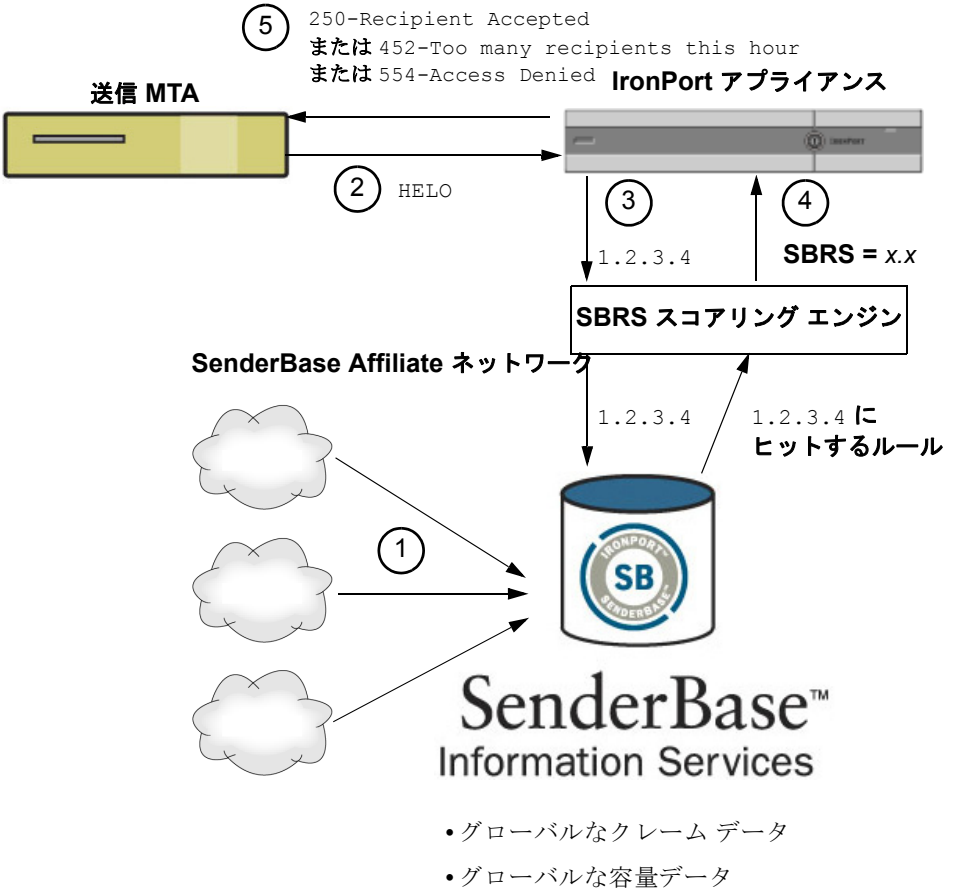
SenderBase Reputation Score（SBRS; SenderBase 評価スコア）は、SenderBase 評価サービスからの情報に基づいて、IP アドレスに割り当てられる数値です。SenderBase 評価サービスは、25 個を超える公開ブラックリストおよびオープン プロキシ リストのデータを集約し、さらにこのデータを SenderBase のグローバル データと組み合わせて、次のように -10.0 ～ +10.0 のスコアを割り当てます。

スコア	意味
-10.0	スパムの送信元である可能性が最も高い
0	中間か、または推奨を行うための十分な情報がない
+10.0	信頼できる送信者である可能性が最も高い

スコアが低いほど、メッセージがスパムである可能性は高くなります。スコアが -10.0 であれば、そのメッセージはスパムであると「保証」されていることを意味し、スコアが 10.0 であれば、そのメッセージは正規であると「保証」されていることを意味します。

SBRS を使用して、信頼性に基づいてメール フロー ポリシーを送信者に適用するように IronPort アプライアンスを設定します（メッセージ フィルタを作成して SenderBase 評価スコアに「しきい値」を指定し、システムで処理されるメッセージにさらにアクションを実行できます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章の「SenderBase Reputation Rule」および「Bypass Anti-Spam System Action」を参照してください）。

図 7-1　SenderBase 評価サービス



ステップ 1　SenderBase Affiliate から、リアルタイムのグローバル データを送信します。

ステップ 2　送信 MTA により、IronPort アプライアンスとの接続が開始されます。

ステップ 3　IronPort アプライアンスにより、接続 IP アドレスのグローバル データがチェックされます。

ステップ 4　SenderBase 評価サービスにより、このメッセージがスパムである可能性が計算され、SenderBase 評価スコアが割り当てられます。

ステップ 5　IronPort により、SenderBase 評価スコアに基づいて応答が返されます。

SenderBase 評価フィルタの実装

SenderBase 評価フィルタ テクノロジーは、IronPort アプライアンスで使用可能なその他のセキュリティ サービスの処理から、できる限り多くのメールを切り離すことを目的としています（「電子メール パイプラインの理解」（P.4-91）を参照）。

評価フィルタリングをイネーブルにすると、既知の悪質な送信者は、単純に拒否されます。世界で 2000 社から送信された既知の良好なメールは、false positive の可能性を低減するために、自動的にフィルタを避けてルーティングされます。未知、または「灰色」の電子メールは、アンチスパム スキャン エンジンにルーティングされます。評価フィルタは、この方法を使用して、コンテンツ フィルタにかかる負荷を最大 50 % 低減できます。

図 7-2　　評価フィルタリングの例

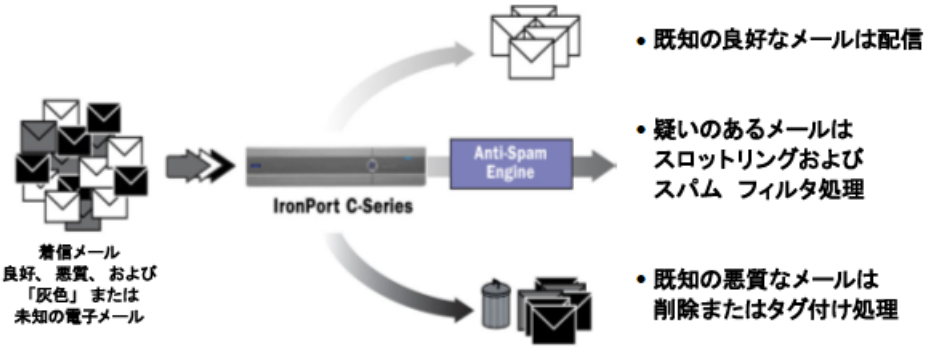


表 7-2 に、SenderBase 評価フィルタリングを実装する場合に推奨されるポリシー セットのリストを示します。企業の目的に応じて、Conservative、Moderate、Aggressive のいずれかの方法を選択できます。

（注）　IronPort ではスロットリングが推奨ですが、SenderBase 評価サービスを実装するもう 1 つの方法として、スパムの疑いのあるメッセージの件名行を変更する方法があります。このようにするには、表 7-1 に示す次のメッセージ フィルタを使用します。このフィルタは、`reputation` フィルタ ルールおよび `strip-header` および `insert-header` フィルタ アクションを使用して、SenderBase 評価スコアが -2.0 未満のメッセージの件名行を、**`{Spam`** ***SBRS}*** のように表現される実際の SenderBase 評価スコアを含む件名行に置き換えます。こ

の例の *listener_name* を、ご使用のパブリック リスナーの名前に置き換えます（このテキストを切り取って `filters` コマンドのコマンドライン インターフェイスに直接貼り付けできるように、この行自体にピリオドが含まれています）。

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

表 7-1　件名ヘッダーを SBRS に変更するメッセージ フィルタ：例 1

```
sbrs_filter:

if ((recv-inj == "listener_name" AND subject != "\\{Spam -?[0-9.]+\\}"))

{

        insert-header("X-SBRS", "$REPUTATION");

        if (reputation <= -2.0)

{

        strip-header("Subject");

        insert-header("Subject", "$Subject \\{Spam $REPUTATION\\}");

       }

 }

.
```

評価フィルタリングの設定

評価フィルタリングは、[Mail Policies] > [HAT Overview] ページで設定します。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。

Conservative

Conservative 方式では、SenderBase 評価スコアが -4.0 未満のメッセージをブロックし、-4.0 ～ -2.0 のメッセージをスロットリングし、-2.0 ～ +6.0 のメッセージにデフォルト ポリシーを適用し、+6.0 を超えるスコアのメッセージに信頼されたポリシーを適用します。この方式を使用すると、false positive 率をほぼ 0 に抑えながら、良好なシステム パフォーマンスを実現できます。

Moderate

Moderate では、SenderBase 評価スコアが -3.0 未満のメッセージをブロックし、-3.0 ～ 0 のメッセージをスロットリングし、0 ～ +6.0 のメッセージにデフォルト ポリシーを適用し、+6.0 を超えるスコアのメッセージに信頼されたポリシーを適用します。この方式を使用すると、false positive 率を非常に低くに抑えながら、良好なシステム パフォーマンスを実現できます（より多くのメールがアンチスパム処理から切り離されるため）。

Aggressive

Aggressive では、SenderBase 評価スコアが -2.0 未満のメッセージをブロックし、-2.0 ～ 0.5 のメッセージをスロットリングし、0 ～ +4.0 のメッセージにデフォルト ポリシーを適用し、+4.0 を超えるスコアのメッセージに信頼されたポリシーを適用します。この方式を使用すると、false positive 率がいくらか発生する可能性はありますが、ほとんどのメールをアンチスパム処理から切り離すことにより、システム パフォーマンスが最大化されます。

（注） また、ユーザは SenderBase 評価スコアが 6.0 より大きいすべてのメッセージを、$TRUSTED ポリシーに割り当てることを推奨します。

表 7-2　SBRS を使用した評価フィルタリング実装の推奨段階的手法

ポリシー	ブラック リスト	スロット リング	デフォルト	ホワイト リスト
Conservative	-10 ～ -4	-4 ～ -2	-2 ～ 7	7 ～ 10
Moderate	-10 ～ -3	-3 ～ -1	-1 ～ 6	6 ～ 10
Aggressive	-10 ～ -2	-2 ～ -0.5	-0.5 ～ 4	4 ～ 10

ポリシー：	特性：	適用するメール フロー ポリシー
Conservative：	false positive はほぼ 0。良好なパフォーマンス。	**$BLOCKED**
Moderate：	false positive は非常に少ない。高パフォーマンス。	**$THROTTLED**
Aggressive：	false positive はいくらか発生。パフォーマンスは最大。	**$DEFAULT**

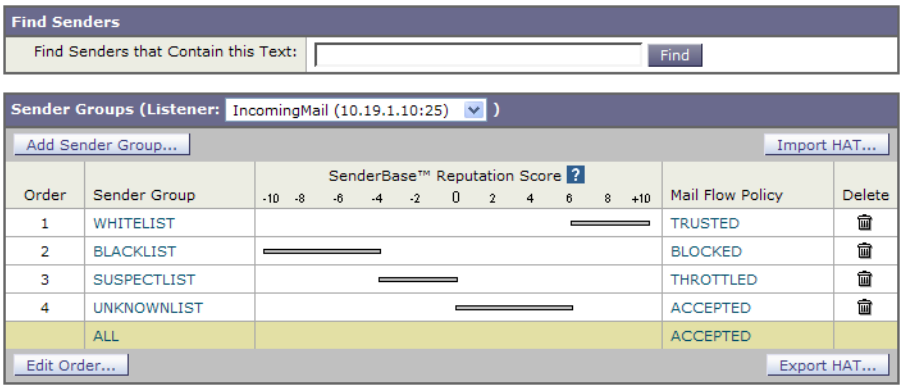
次の手順では、評価フィルタリングを実装する段階的手法の概要を示します。

リスナーの HAT での評価フィルタリング実装

パブリック リスナーのデフォルト HAT エントリを編集して、SBRS を含めるには、次の手順を実行します。

ステップ 1　[Mail Policies] タブで、[Host Access Table] > [HAT Overview] を選択します。[Sender Groups (Listener)] メニューからパブリック リスナーを選択します。[HAT Overview] ページに、各送信者グループの SenderBase 評価スコア設定が表示されます。

図 7-3　送信者グループの SenderBase 評価スコア範囲リスト

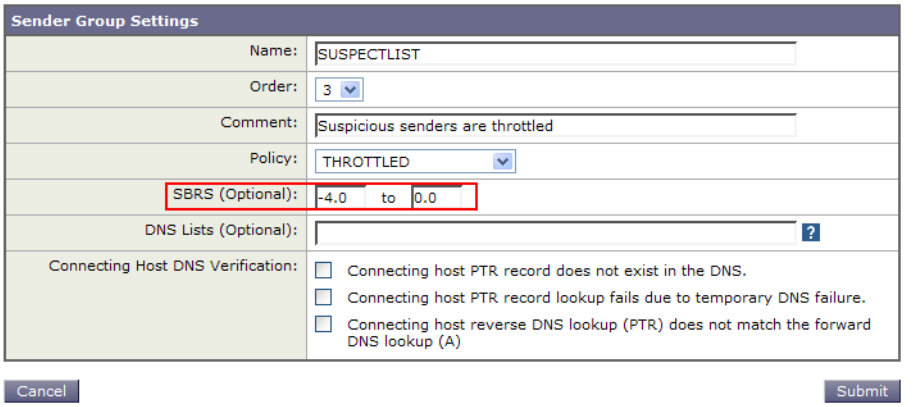


[HAT Overview] には、各送信者グループ（水平バー）に割り当てられた SenderBase 評価スコアの範囲および関連付けられたメール フロー ポリシーが表示されます。

ステップ 2　送信者グループのリンクをクリックします。

たとえば、「SUSPECTLIST」のリンクをクリックします。[Edit Sender Group] ページが表示されます。

図 7-4　送信者グループの SBRS 範囲



ステップ 3　SenderBase 評価スコアの範囲を入力して、送信者グループを定義します。任意でコメントを定義することもできます。

たとえば、「SUSPECTLIST」に -4.0 ～ 0 の範囲を入力します。構文については、「SenderBase 評価スコアによって定義された送信者グループ」（P.5-136）を参照してください。

ステップ 4　[Submit] をクリックします。

リスナーの HAT で、各グループについて手順 2 ～ 5 を繰り返します。たとえば、*conservative* 方式の値を定義します。表 7-2 に示した Moderate または Aggressive 方式の値も定義できます。

送信者グループ	SBRS Range	メール フロー ポリシー
WHITELIST	6 ～ 10	TRUSTED
BLACKLIST	-10 ～ -7	BLOCKED

送信者グループ	SBRS Range	メール フロー ポリシー
SUSPECTLIST	-7 ～ -2	THROTTLED
UNKOWNLIST	-2 ～ 6	ACCEPTED

（注）　リスナーの HAT で送信者グループを定義するときは、順序に注意してください（リスナーへの接続を試行する各ホストで、HAT は上から下へ順に読み込まれます。接続ホストにルールが一致すると、その接続に対してただちにアクションが実行されます）。IronPort では、リスナーの HAT であらかじめ定義されている送信者グループをデフォルトの順序で維持すること（つまり、RELAYLIST（C150/160 カスタマーのみ）、WHITELIST、BLACKLIST、SUSPECTLIST、UNKNOWNLIST の順）を推奨します。

ステップ 5　[Commit Changes] ボタンをクリックし、必要に応じて任意のコメントを追加してから [Commit Changes] をクリックして、リスナーの HAT での評価フィルタリングの実装を終了します。

SBRS を使用した評価フィルタリングのテスト

常時大量のスパムを受信しているか、または組織に対するスパムを受信するために「ダミー」のアカウントを特に設定していない限り、実装した SBRS ポリシーをただちにテストすることは困難です。ただし、表 7-3 に示すように、リスナーの HAT に SenderBase 評価スコアによる評価フィルタリングのエントリを追加した場合は、インバウンド メールのうち「未分類」になるパーセンテージが低くなります。

作成したポリシーは、任意の SBRS で trace コマンドを使用してテストします。Debugging Mail Flow Using Test Messages: Trace, page -446 を参照してください。trace コマンドは、GUI だけでなく CLI でも使用できます。

表 7-3　SBRS 実装の推奨メール フロー ポリシー

ポリシー名	主要な動作（アクセス ルール）	パラメータ	値
$BLOCKED	REJECT	None	
$THROTTLED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Maximum recipients / hour: Use SenderBase:	10 20 1 MB 10 ON OFF **20** *（推奨）* ON
$ACCEPTED（パブリック リスナー）	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Use SenderBase:	1,000 1,000 100 MB 1,000 ON OFF ON
$TRUSTED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Maximum recipients / hour: Use SenderBase:	1,000 1,000 100 MB 1,000 OFF OFF -1 *（ディセーブル）* OFF

（注）　$THROTTLED ポリシーでは、リモート ホストから受信する 1 時間あたりの最大受信者数は、デフォルトで 1 時間あたり 20 人に設定されています。この設定により、使用可能な最大スロットリングが制御されることに注意してください。このパラメータが厳しすぎる場合は、時間あたりの受信者数を増やすことができます。デフォルトのホスト アクセス ポリシーの詳細については、「パブリック リスナー向けの定義済みのメール フロー ポリシー」（P.5-139）を参照してください。

SenderBase 評価サービスのステータスのモニタリング

[Security Services] メニューの [SenderBase] ページには、IronPort アプライアンスから SenderBase Network Status Server および SenderBase 評価スコア サービスに対して最後に実行したクエリーの接続ステータスおよびタイムスタンプが表示されます。SenderBase 評価スコア サービスは、アプライアンスに SRBS スコアを送信します。SenderBase Network Server は、アプライアンスにメール送信元の IP アドレス、ドメイン、および組織などの情報を送信します。AsyncOS は、このデータをレポート作成および電子メール モニタリング機能に使用します。

図 7-5　[SenderBase] ページの [SenderBase Network Status]

SenderBase Network Status		
Type	Status	Last Status Check
SenderBase Network Server	up	Wed Sep 10 13:44:52 2008 PDT
SenderBase Reputation Score Service	up	Wed Sep 10 13:44:52 2008 PDT

CLI の `sbstatus` コマンドでも、同じ情報を表示できます。