送信者レピュテーション フィルタリング

この章は、次の項で構成されています。

- 送信者レピュテーション フィルタリングの概要 （1 ページ）
- SenderBase レピュテーション サービス （1 ページ）
- リスナーの送信者レピュテーション フィルタリング スコアのしきい値の編集 （5 ページ）
- メッセージの件名への低い SBRS スコアの入力 （7 ページ）

送信者レピュテーション フィルタリングの概要

送信者レピュテーション フィルタリングは、スパム保護の最初のレイヤで、Cisco SenderBase™ レピュテーション 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 ゲートウェイ経由で送信されるメッセージを制御できます。

アプライアンスは、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を受け取り、コンテンツ スキャンを一切実施しないでエンドユーザに直接配信できます。未知または信頼性の低い送信者からのメッセージは、アンチスパムおよびアンチウイルス スキャンなどのコンテンツ 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。

（注） ファイル レピュテーション フィルタリングは別のサービスです。詳細については、次の資料を参照してください。 ファイル レピュテーション フィルタリングとファイル分析

SenderBase レピュテーション サービス

SenderBase Affiliate ネットワークからのグローバル データを使用する Cisco SenderBase レピュテーション サービスは、クレーム率、メッセージ量の統計情報、および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に基づいて、電子メール送信者に SenderBase レピュテー

ション スコアを割り当てます。SenderBase レピュテーション スコア サービスは、正当な送信者とスパム発信元を区別する際に役立ちます。レピュテーション スコアの低い送信者からのメッセージをブロックするしきい値を指定することも可能です。

SenderBase Security Network Web サイト（www.senderbase.org）では、最新の電子メールおよびWebベースの脅威のグローバルな概要を提供し、国別の電子メール トラフィック量を表示し、IP アドレス、URI、またはドメインに基づいたレピュテーション スコアを検索できます。

（注） SenderBase レピュテーション サービスは、現在のスパム対策ライセンス キー以外では使用できません。

SenderBase レピュテーション スコア（SBRS）

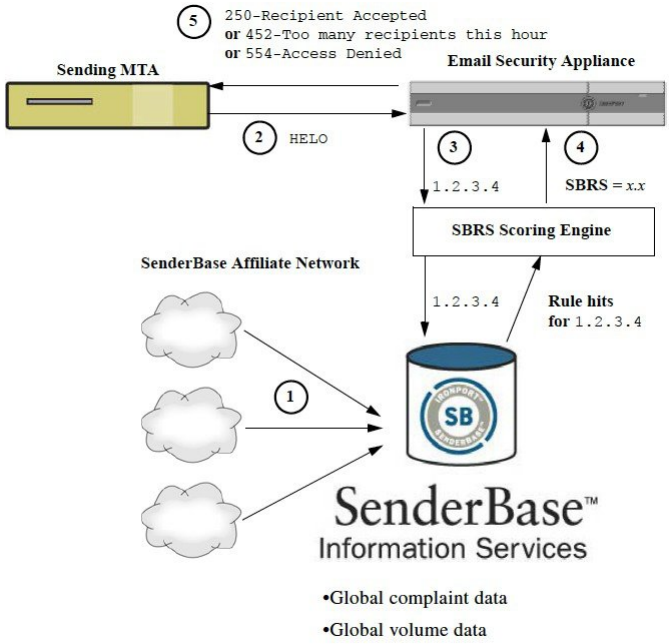
SenderBase レピュテーション スコア（SBRS）は、SenderBase レピュテーション サービスからの情報に基づいて、IPアドレスに割り当てられる数値です。SenderBase レピュテーション サービスは、25個を超える公開ブラックリストおよびオープンプロキシリストのデータを集約し、さらにこのデータをSenderBaseのグローバルデータと組み合わせて、次のように-10.0～+10.0のスコアを割り当てます。

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 レピュテーション 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、SenderBase レピュテーション ルールおよびアンチスパム システムのバイパス アクションを参照してください）。

図 *1 : SenderBase* レピュテーション サービス



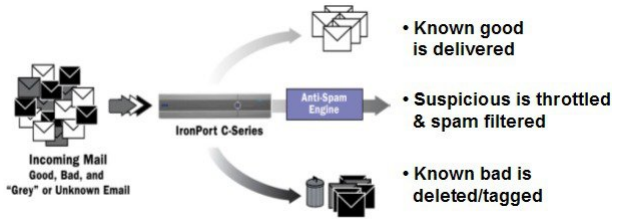
1. SenderBase Affiliate から、リアルタイムのグローバル データを送信します。
2. 送信側 MTA により、アプライアンスとの接続が開始されます。
3. アプライアンスにより、接続 IP アドレスのグローバル データがチェックされます。
4. SenderBase レピュテーション サービスにより、このメッセージがスパムである可能性が計算され、SenderBase レピュテーション スコアが割り当てられます。
5. シスコ により、SenderBase レピュテーション スコアに基づいて応答が返されます。

SenderBase レピュテーション フィルタの仕組み

送信者レピュテーション フィルタ テクノロジーは、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 パイプラインについて を参照）。

送信者レピュテーションフィルタリングがイネーブルになっている場合は、既知の悪質な送信者からのメールだけが拒否されます。世界中の 2000 社から送信された既知の良好なメールは自動的にスパム フィルタを避けてルーティングされるため、誤検出の可能性が低減されます。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。送信者レピュテーション 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 *2:* 送信者レピュテーション フィルタリングの例



さまざまな送信者レピュテーション フィルタリング手法の推奨設定

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。

アプローチ	特性	WHITELIST	BLACKLIST	SUSPECTLIST	UNKNOWNLIST
		SenderBase レピュテーション スコア範囲			
Conservative	誤検出はほぼ 0。良好なパフォーマンス。	7 ～ 10	-10 ～ -4	-4 ～ -2	-2 ～ 7
Moderate（インストール時のデフォルト）	誤検出は非常に少ない。高パフォーマンス。	SenderBase レピュテーション スコアは使用されません。	-10 ～ -3	-3 ～ -1	-1 ～ +10
Aggressive	誤検出はいくらか発生。パフォーマンスは最大。 このオプションは、ほとんどのメールをアンチスパム処理から切り離します。	4 ～ 10	-10 ～ -2	-2 ～ -1	-1 ～ 4
すべての方式		**メール フロー ポリシー**：			
		信頼できる	ブロック	スロットル	承認（Accepted）

リスナーの送信者レピュテーションフィルタリングスコアのしきい値の編集

デフォルトの SenderBase レピュテーション サービス（SBRS）スコアのしきい値を変更またはレピュテーション フィルタリングに送信者グループを追加する場合は、この手順を使用します。

（注） SBRS スコアのしきい値に関連するその他の設定およびメール フロー ポリシー設定については、次に記載されています ホスト アクセス テーブルを使用した接続を許可するホストの定義

はじめる前に

- 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 ホストを特定してください。詳細については、着信リレー構成における送信者の IP アドレスの決定を参照してください。
- SenderBase レピュテーション スコア範囲について理解します。SenderBase レピュテーション スコアを使用した送信者グループの定義を参照してください。
- 組織のフィルタリング方法を選択し、このアプローチの推奨設定を確認します。さまざまな送信者レピュテーション フィルタリング手法の推奨設定 （4 ページ）を参照してください。

ステップ 1 [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] を選択します。

ステップ 2 [送信者グループ（リスナー）（Sender Groups (Listener)）] メニューからパブリック リスナーを選択します。

ステップ 3 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。

ステップ 4 [設定の編集（Edit Settings）] をクリックします。

ステップ 5 送信者グループの SenderBase レピュテーション スコアの範囲を入力します。

たとえば、「WHITELIST」に 7.0 ～ 10 の範囲を入力します。

ステップ 6 [送信（Submit）] をクリックします。

ステップ 7 必要に応じてこのリスナーの各送信者グループに対し、繰り返し実行します。

ステップ 8 変更を確定します。

SBRS を使用した送信者レピュテーション 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、次の表に示すように、リスナーの HAT に SenderBase レピュテーション スコアによるレピュテーション 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。

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。テスト メッセージを使用したメール フローのデバッグ：トレース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 *1 : SBRS* 実装の推奨メール フロー ポリシー

ポリシー名	主な動作（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 オン オフ **20**（推奨） オン
`$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 オン オフ オン

ポリシー名	主な動作（アクセス ルール）	パラメータ	値
$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 オフ オフ -1（ディセーブル） オフ

（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、定義済みの送信者グループとメール フロー ポリシーの理解を参照してください。

SenderBase レピュテーション サービスのステータスのモニタリング

SenderBase レピュテーション 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、および組織について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。

これらのサービスへの接続のステータスを表示するには、[セキュリティ サービス（Security Services）] > [SenderBase] を選択します。

[セキュリティサービス（Security Services）] メニューの [SenderBase] ページには、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。

CLI で `sbstatus` コマンドを使用しても、同じ情報を表示できます。

メッセージの件名への低い SBRS スコアの入力

スロットリングを推奨しますが、SenderBase レピュテーション サービスを使用する別方法では、スパムの疑いのあるメッセージの件名行を変更します。これを行うには、次の表に示すメッセージ 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 レピュテーション 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 レピュテーション 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）。

表：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\\}");

       }

 }

.
```

関連項目

- メッセージ フィルタを使用した電子メール ポリシーの適用