IP 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 IP レピュテーション フィルタリングの概要

送信者 IP レピュテーション フィルタリングは、スパム対策の最初のレイヤです。の送信者 IP 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。

電子メールゲートウェイは、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。

Note 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、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を参照してください。

IP レピュテーションサービス

Talos 関係会社のネットワークからのグローバルデータを使用する IP 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、および公開ブロ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 IP レピュテーションスコア（IPRS）を割り当てます。IP レピュテーションスコアは、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。

Talos セキュリティネットワーク Web サイト（https://talosintelligence.com）では、最新の電子メールおよび Web ベースのグローバルな脅威の概要を提供し、現在の電子メールトラフィック量を国別に表示します。また、IP アドレス、URI、またはドメインに基づいてレピュテーションスコアを検索できます。

関連項目

- IP レピュテーションスコア , on page 2
- 送信者 IP レピュテーションフィルタの仕組み , on page 3
- さまざまな送信者 IP レピュテーション フィルタリング手法の推奨設定 , on page 4
- アウトブレイク フィルタ
- 電子メール セキュリティ モニタの使用方法

IP レピュテーションスコア

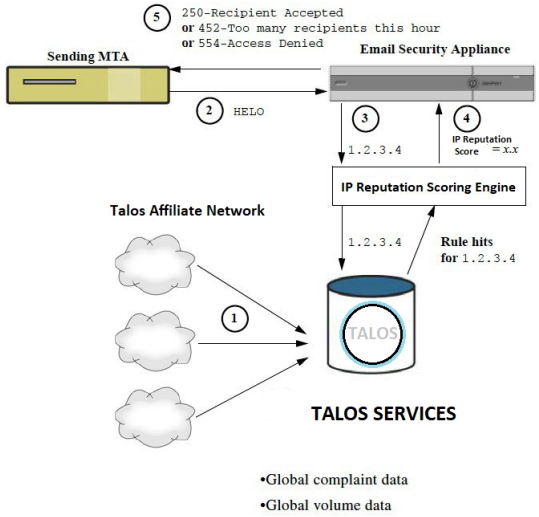
IP レピュテーションスコアは、IP レピュテーションサービスからの情報に基づいて、IP アドレスに割り当てられる数値です。IP レピュテーションサービスは、25 個を超える公開ブロックリストおよびオープンプロキシリストのデータを集約し、さらにこのデータを Talos のグローバルデータと組み合わせて、次のように -10.0 ～ +10.0 のスコアを割り当てます。

スコア（Score）	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。

IP レピュテーションスコアを使用して、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電子メールゲートウェイを設定します。メッセージフィルタを作成して IP 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、IP 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）。

Figure 1: IP レピュテーションサービス



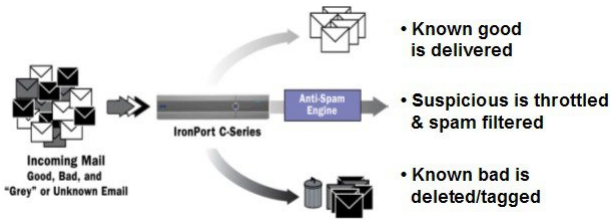
1. Talos 関連会社から、リアルタイムのグローバル データを送信します。
2. 送信側 MTA により、 電子メールゲートウェイとの接続が開始されます。
3. 電子メールゲートウェイにより、接続 IP アドレスのグローバルデータがチェックされます。
4. IP レピュテーションサービスにより、このメッセージがスパムである可能性が計算され、IP レピュテーションスコアが割り当てられます。
5. シスコにより、IP レピュテーションスコアに基づいて応答が返されます。

送信者 IP レピュテーションフィルタの仕組み

送信者 IP レピュテーション フィルタ テクノロジーは、電子メールゲートウェイに搭載されている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 IP 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。

Figure 2: 送信者 *IP* 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 IP 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	Allowed _List	Blocked_ List	SUSPECTLIST	UNKNOWNLIST
		送信者 IP 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。	送信者 IP 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
アグレッシブ	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 IP 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 IP レピュテーションサービス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。

Note IP レピュテーション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の設定については、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に記載されています。

はじめる前に

- 電子メールゲートウェイがローカル 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。
- IP レピュテーションスコアについて理解します。IP 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 IP レピュテーション フィルタリング手法の推奨設定 , on page 4を参照してください。

Procedure

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 IP レピュテーションスコアの範囲を入力します。

たとえば、「ALLOWED_LIST」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。

What to do next

関連項目

- IP レピュテーションスコアを使用したIP レピュテーション フィルタリングのテスト, on page 5
- 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
- メッセージがスパムかどうかスキャンするための 電子メールゲートウェイの設定方法

IP レピュテーションスコアを使用したIP 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 IP レピュテーション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 IP 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、受信メールのうち「未分類」になるパーセンテージが低くなります。

このポリシーは、任意の IP レピュテーションスコアを指定し、`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。

***Table 1: IP* レピュテーションスコア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
`$ACCEPTED` （パブリック リスナー）	`ACCEPT`	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Use SenderBase:	1,000 1,000 100 MB 1,000 オン オフ 点灯
`$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 消灯 -1（無効） OFF

Note $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。

メッセージサブジェクトへの低IPレピュテーションスコアの入力

スロットリングを推奨しますが、IP レピュテーションサービスを使用して、スパムの疑いのあるメッセージの件名行を変更するという別の方法もあります。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、strip-header および insert-header フィルタアクションを使用して、IP 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実際の IP レピュテーションスコアを含む件名行に置き換えます。**{Spam *IP Reputation Score*}** のように表されます。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 IP レピュテーション に変更するメッセージフィルタ：例 1

```
iprs_filter:

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

{

        insert-header("X-IPRS", "$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