スパムおよびグレイメールの管理

この章は、次の項で構成されています。

スパム対策スキャンの概要

スパム対策プロセスは、設定するメールポリシーに基づいて着信（および発信）のメールの電子メールをスキャンします。

- 1 つ以上のスキャン エンジンはフィルタ モジュールによってメッセージをスキャンします。
- スキャン エンジンは、各メッセージにスコアを割り当てます。スコアが高いほど、メッセージがスパムである可能性が高くなります。
- スコアに基づいて、各メッセージは次のいずれかに分類されます。
  - スパムではない電子メール
  - スパムだと疑われる電子メール
  - 陽性と判定されたスパム
- 結果に基づいてアクションが実行されます。

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 メッセージとして識別されたメッセージに対して実行されるアクションは、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の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 メッセージを隔離する必要がある場合があります。

各メールポリシーで、カテゴリの複数のしきい値を指定し、各カテゴリに対して実行するアクションを指定できます。異なるメールポリシーに異なるユーザを割り当て、各ポリシーに対して異なるスキャン エンジン、スパム定義しきい値、スパム処理アクションを定義できます。

（注） スパム対策スキャンの適用方法および適用時期の詳細については、電子メール パイプラインとセキュリティ サービスを参照してください。

関連項目

- スパム対策ソリューション （2 ページ）

スパム対策ソリューション

アプライアンス は次のスパム対策ソリューションを提供します。

- IronPort スパム対策フィルタリング （4 ページ）。
- Intelligent Multi-Scan とグレイメール検出の設定 （8 ページ）。

アプライアンスの両方のソリューションを認可して有効にできますが、特定のメールポリシーでは1つしか使用できません。ユーザのグループごとに異なるスパム対策ソリューションを指定できます。

メッセージがスパムかどうかスキャンするためのアプライアンス の設定方法

手順

	コマンドまたはアクション	目的
ステップ 1	アプライアンスのスパム対策スキャニングをイネーブルにします。	（注） この表の残りの手順は、両方のスキャン エンジンにオプションに適用されます。

	コマンドまたはアクション	目的
		Cisco IronPort Anti-Spam および Intelligent Multi-Scan の両方のライセンスキーがある場合は、アプライアンスの両方のソリューションをイネーブルにできます。 • IronPort スパム対策フィルタリング（4 ページ） • Intelligent Multi-Scan とグレイメール検出の設定 （8 ページ）
ステップ 2	ローカルのアプライアンスからスパムを隔離するか、セキュリティ管理アプライアンスの外部隔離を使用するかどうかを設定します。	• ローカルのスパム隔離の設定 • 外部スパム隔離の操作
ステップ 3	メッセージのスパムをスキャンするユーザ グループを定義します。	送信者および受信者のグループのメール ポリシーの作成
ステップ 4	定義したユーザ グループのスパム対策スキャン ルールを設定します。	スパム対策ポリシーの定義 （22 ページ）
ステップ 5	特定のメッセージに対する Cisco Anti-Spam スキャンをスキップし、skip-spamcheck アクションを使用するメッセージ フィルタを作成します。	アンチスパム システムのバイパス アクション
ステップ 6	（推奨）IP レピュテーションスコアに基づいて接続を拒否しない場合でも、IP レピュテーションスコアを各受信メールフローポリシーで有効にします。	各受信メール フロー ポリシーで、[フロー制御にSenderBaseを使用（Use SenderBase for Flow Control）] がオンになっていることを確認します。 「メール フロー ポリシーを使用した着信メッセージのルールの定義」を参照してください。
ステップ 7	アプライアンスが着信電子メールを受信するために外部送信者に直接接続しない代わりに、メール交換、メール転送エージェント、ネットワークの他のマシンからリレーされたメッセージを受信する場合は、リレーされた着信メッセージに元の送信者の IP アドレスが含まれていることを確認します。	着信リレー構成における送信者の IP アドレスの決定 （37 ページ）

	コマンドまたはアクション	目的
ステップ 8	アプライアンスで生成されたアラートや他のメッセージがスパムとして間違って識別されないようにします。	スパムフィルタからのアプライアンス生成メッセージの保護 （30 ページ）
ステップ 9	（任意）メッセージ内の悪意のある URL に対する保護を強化するため、URL フィルタリングをイネーブルにします。	URL フィルタリングを有効にする
ステップ 10	設定をテストします。	スパム対策のテスト （48 ページ）
ステップ 11	（任意）サービスの更新を設定します（スパム対策ルールも含め）。	両方のスパム対策ソリューションのスキャン ルールが Cisco 更新サーバからデフォルトで取得されます。 • サービス アップデート • プロキシサーバを経由したアップデート • アップグレードおよびアップデートをダウンロードするためのサーバ設定

IronPort スパム対策フィルタリング

関連項目

- 評価キー （4 ページ）
- Cisco Anti-Spam：概要 （5 ページ）
- IronPort Anti-Spam スキャンの設定 （6 ページ）

評価キー

アプライアンス には、Cisco 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、システム セットアップ ウィザードまたは [セキュリティサービス（Security Services）] > [IronPort Anti-Spam] ページ（GUI）か、systemsetup コマンドまたは antispamconfig 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 Cisco Anti-Spam がイネーブルになります。設定した管理者アドレス（システム設定ウィザード、手順 2：システムを参照）に対して、Cisco 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有効にする場合の詳細については、Cisco 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、[システム管理（System Administration）] > [ライセンスキー（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、ライセンス キーを参照してください。）

Cisco Anti-Spam：概要

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。

これらの脅威を特定するには、IronPort Anti-Spam はそのメッセージ コンテンツの完全なコンテキスト、メッセージの構築方法、送信者のレピュテーション、メッセージでなどによりアドバタイズされる Web サイトのレピュテーションを検査します。IronPort Anti-Spam は世界最大の電子メールおよび Web モニタリング ネットワークである SenderBase を最大限に活用する電子メールおよび Web レピュテーション データを組み合わせ、開始と同時に新しい攻撃を検出します。

IronPort Anti-Spam は次の分野における 100,000 以上のメッセージ属性を分析します。

- 電子メール レピュテーション：このメッセージの送信者は誰か。
- 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。
- 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。
- Web レピュテーション：遷移先はどこか。

多次元的な関係を分析することにより、精度を維持しながら、システムは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、肯定的なレピュテーション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。

関連項目

- 国際地域のスパムのスキャン （5 ページ）
- URL 関連の保護および制御

国際地域のスパムのスキャン

Cisco Anti-Spam は世界的に有効な、ロケール固有コンテンツ対応の脅威検出技術を使用します。また、リージョナル ルール プロファイルを使用して特定の地域のスパム対策スキャンを最適化できます。

- 米国以外の特定の地域から大量のスパムを受信すると、リージョナル ルール プロファイルを使用してその地域のスパムを停止することもできます。

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、香港のメールを受信する場合、シスコでは、スパム対策エンジンに含まれる中国のリージョナル ルール プロファイルを使用することを強く推奨しています。

- スパムが米国または他の特定の地域から主に来る場合、スパムの他のタイプの検出率を低下する可能性があるため、リージョナル ルールをイネーブルにしないでください。これは、リージョナル ルール プロファイルが特定地域向けスパム対策エンジンを最適化するためです。

IronPort Anti-Spam スキャンを設定するときにリージョナル ルール プロファイルをイネーブルにできます。

関連項目

- IronPort Anti-Spam スキャンの設定 （6 ページ）

IronPort Anti-Spam スキャンの設定

（注） IronPort Anti-Spam をシステム セットアップ時に有効にすると、グローバル設定のデフォルト値を使用し、デフォルトの着信メール ポリシーで有効にされます。

はじめる前に

- リージョナル スキャンを使用するかどうかを設定します。国際地域のスパムのスキャン（5 ページ）を参照してください。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [IronPort Anti-Spam] を選択します。

ステップ 2 システム セットアップ ウィザードで [IronPort Anti-Spam] をイネーブルにしなかった場合：

a) **[有効（Enable）]** をクリックします。

b) ライセンス契約書ページの下部にスクロールし、[承認（Accept）] をクリックしてライセンス契約に合意します。

ステップ 3 **[グローバル設定を編集（Edit Global Settings）]** をクリックします。

ステップ 4 [IronPort Anti-Spamスキャニングを有効にする（Enable IronPort Anti-Spam Scanning）] チェックボックスを選択します。

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。

ステップ 5 スパム送信者から続々と送信される大量メッセージをスキャンする能力を備えながらも、アプライアンス のスループット最適化を図るため、Cisco Anti-Spam によるメッセージスキャンのしきい値を設定します。

オプション	説明
メッセージのスキャンのしきい値（Message Scanning Thresholds）	**1.** [次のサイズより小さい場合は常にメッセージをスキャン（Always scan messages smaller than）] に値を入力します。推奨値は 1 MB 以下です。「初期終了」の場合を除き、*always scan* サイズより小さいメッセージは完全にスキャンします。このサイズより大きいメッセージは、never scan サイズより小さい場合、部分的にスキャンします。 *always scan* メッセージ サイズは 3 MB を超えないようにしてください。値が大きくなると、パフォーマンスが低下する可能性があります。 **2.** [次のサイズより大きい場合はメッセージをスキャンしない（Never scan messages larger than）] に値を入力します。推奨値は 2 MB 以下です。このサイズより大きいメッセージは Cisco 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。 *never scan* メッセージ サイズは 10 MB を超えないようにしてください。値が大きくなると、パフォーマンスが低下する可能性があります。 *always scan* サイズより大きいか、または *never scan* サイズより小さいメッセージについては、限定的な高速スキャンを実行します。 （注） アウトブレイク フィルタの最大メッセージ サイズが Cisco Anti-Spam の always scan メッセージよりも大きい場合、アウトブレイク フィルタの最大サイズよりも小さいメッセージは完全にスキャンされます。
1 つのメッセージのスキャンのタイムアウト（Timeout for Scanning Single Message）	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。 1 ～ 120 の整数を入力します。デフォルト値は 60 秒です。

オプション	説明
スキャンプロファイル（Scanning Profile）	スパム メッセージを捕捉するには、次のスキャン プロファイルのいずれかを選択します。 • 通常（Normal）：スパムをブロックするためのバランスの取れたアプローチを使用するには、このオプションを有効にします。 • アグレッシブ（Aggressive）：スパムのブロックを強化するには、このオプションを有効にします。有効にすると、スパム対策ポリシーしきい値を調整したときに、[通常（Normal）]プロファイルよりも、スパム検出に対する影響が大きくなり、誤検出の可能性が高くなります。 （注） 新しいアグレッシブ スキャンプロファイルを使用している場合、メールポリシーを調整してスパム対策のしきい値を変更すると、以前よりも与える影響が大きくなります。したがって、アグレッシブプロファイルを有効にする際、以前に調整したスパム対策ポリシーのしきい値がある場合はデフォルト設定にリセットし、スパム検出率と誤検出の可能性のバランスが最適になるように再評価する必要があります。 • リージョン（中国）（Regional (China)）：指定した地域から大量の電子メールを受信する場合にのみこの機能を有効にします。サポートされている地域は中国です。このオプションでは特定のリージョンに合わせてスパム対策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。

ステップ 6 変更を送信し、保存します。

Intelligent Multi-Scan とグレイメール検出の設定

このセクションでは、Cisco Intelligent Multi-Scan と、グレイメール検出および安全な配信停止を設定する方法を説明します。

• Cisco Intelligent Multi-Scan の設定 （9 ページ）
• Intelligent Multi-Scan とグレイメール検出のグローバル設定 （21 ページ）
• グレイメールの管理 （10 ページ）

Cisco Intelligent Multi-Scan の設定

Cisco Intelligent Multi-Scan では、Cisco Anti-Spam を含めた複数のスキャン対策エンジンを組み込むことにより、多層スパム対策ソリューションを実現しています。

Cisco Intelligent Multi-Scan によって処理された場合：

- メッセージは、サードパーティ製スパム対策エンジンによって最初にスキャンされます。
- Cisco Intelligent Multi-Scan は次に、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を Cisco Anti-Spam に渡し、最終判定が下されます。
- Cisco Anti-Spam がスキャンを実行した後、結合された複数のスキャン スコアを AsyncOS に返します。
- Cisco Anti-Spam の低い誤検出率を維持したまま、サードパーティ製スキャン エンジンおよびシスコのスパム対策の結果を組み合わせることで、より多くのスパムが検出されます。

Cisco 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。Cisco 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 Cisco Intelligent Multi-Scan がスキップすることはありません。

Cisco 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、シスコのサポート担当者にお問い合わせください

（注） Cisco Intelligent Multi-Scan 機能キーによって、アプライアンス で Cisco Anti-Spam も有効になります。その結果、メールポリシーで Cisco Intelligent MultiScan または Cisco Anti-Spam のいずれかを有効にできるようになります。

重要 Cisco Intelligent Multi-Scan をシステム セットアップ時にイネーブルにすると、グローバル設定のデフォルト値を使用し、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。

始める前に

この機能のライセンス キーをアクティブにします。ライセンス キーを参照してください。これを行った場合にだけ [IronPortインテリジェントマルチスキャン（IronPort Intelligent Multi-Scan）] オプションが表示されます。

手順

ステップ 1 **[セキュリティサービス（Security Services）] > [IMSおよびグレイメール（IMS and Graymail）]** を選択します。

ステップ 2 システム セットアップ ウィザードで Cisco Intelligent Multi-Scan をイネーブルにしていない場合：

a) **[有効（Enable）]** をクリックします。

b) ライセンス契約書ページの下部にスクロールし、[承認（Accept）] をクリックしてライセンス契約に合意します。

ステップ 3 [IMS設定の編集（Edit IMS Settings）] をクリックします。

ステップ 4 [Intelligent Multi-Scanの有効化（Enable Intelligent Multi-Scan）] のチェックボックスをオンにして、アプライアンス 全体で機能を有効化します。ただし、メール ポリシーの受信者ごとの設定値は依然として有効にする必要があります。

ステップ 5 （任意）[グローバル設定の編集（Edit Global Settings）] をクリックして、メッセージ スキャンのしきい値を設定します。グローバル設定の詳細については、Intelligent Multi-Scan とグレイメール検出のグローバル設定 （21 ページ） を参照してください。

ステップ 6 変更を送信し、保存します。

グレイメールの管理

グレイメールの概要

グレイメール メッセージとは、ニュースレター、メーリング リストのサブスクリプション、ソーシャル メディア通知など、スパムの定義に適合しないメッセージです。これらのメッセージは、ある時点では役に立ちますが、その後エンドユーザがもはや受信したくないところまで価値が減少します。

グレイメールとスパムの違いは、エンドユーザが購読していないメッセージであるスパムと異なり、いずれかの時点（エンド ユーザが e-コマース Web サイトでニュースレターを購読したり、会議中に組織に連絡先詳細を提供した場合など）でエンド ユーザが意図的に電子メール アドレスを提供した点です。

E メール セキュリティ アプライアンス でのグレイメール管理ソリューション

アプライアンス のグレイメール管理ソリューションは、統合されたグレイメール スキャン エンジンとクラウドベースの登録解除サービスの 2 つのコンポーネントで構成されます。

組織でグレイメール管理ソリューションを使用すると、以下が可能になります。

- 統合グレイメールエンジンを使用してグレイメールを識別し、適切なポリシー制御を適用します。
- 登録解除サービスを使用して、不要なメッセージを配信停止にする簡単なメカニズムをエンドユーザに提供します。

これらに加えて、グレイメール管理ソリューションでは、組織に以下を提供することもできます。

- **エンドユーザへの安全な配信停止オプション。**配信停止オプションを模倣することは、よくあるフィッシング技法です。そのため、一般にエンドユーザは、不明な購読解約リンクのクリックに慎重になります。このようなシナリオでは、クラウドベースの登録解除サービスが元の配信停止URIを抽出し、URIのレピュテーションをチェックして、エンドユーザに代わって配信停止プロセスを実行します。これにより、配信停止リンクを装った悪意のある脅威からエンドユーザを保護します。
- **エンドユーザを対象として統一されたサブスクリプション管理インターフェイス。**さまざまなグレイメール送信者が、ユーザに配信停止リンクを表示するためのさまざまなレイアウトを使用しています。ユーザは、メッセージ本文で配信停止リンクを探して、配信停止を行う必要があります。グレイメール送信者に関係なく、グレイメール管理ソリューションは、配信停止リンクを表示するための共通のレイアウトを提供します。
- **管理者にさまざまなグレイメールカテゴリに対するより良い可視性を提供。**グレイメールエンジンでは、各グレイメールを3つのカテゴリに分類し（グレイメールの分類（11ページ）を参照）、管理者はこれらのカテゴリに基づいてポリシー制御を設定できます。
- **スパムに対する有効性の改善**

関連項目

- グレイメールの分類 （11 ページ）

グレイメールの分類

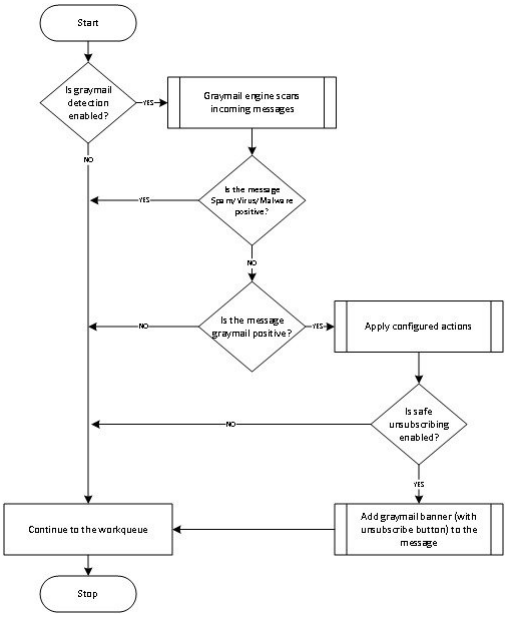
グレイメール エンジンでは、各グレイメールを次のいずれかのカテゴリに分類します。

- **マーケティング メール。**Amazon.com からの新たに販売される製品の詳細に関する記事など、プロフェッショナル マーケティング グループから送信された広告メッセージ。
- **ソーシャル ネットワーク メール。**ソーシャル ネットワーク、出会い系/結婚 Web サイト、フォーラムなどからの通知メッセージ。例として、以下からのアラートなどが挙げられます。
  - LinkedIn。関心があると思われるジョブについて
  - CNET Forum。ユーザが投稿に応答した場合。
- **バルク メール。**認識されないマーケティング グループから送信された広告メッセージ（テクノロジー メディア企業の TechTarget からのニュースレターなど）。

グレイメール管理ソリューションの仕組み

次の手順では、グレイメール管理ソリューションのワークフローを示します。

図 *1:* グレイメール管理ソリューションのワークフロー



ワークフロー（Workflow）

手順

ステップ 1 アプライアンス は、着信メッセージを受信します。

ステップ 2 アプライアンスは、グレイメール検出が有効かどうかを確認します。グレイメール検出が有効になっている場合は、ステップ 3 に進みます。それ以外の場合は、ステップ 8 に進みます。

ステップ 3 アプライアンスは、メッセージがスパム、ウイルス、またはマルウェア陽性かどうかを確認します。陽性の場合は、ステップ 8 に進みます。それ以外の場合は、ステップ 4 に進みます。

ステップ 4 アプライアンス は、メッセージがグレイメールかどうかを確認します。メッセージがグレイメールの場合は、ステップ 5 に進みます。それ以外の場合は、ステップ 8 に進みます。

ステップ 5 アプライアンスは、削除、配信、バウンス、スパム隔離エリアへの隔離など、設定されたポリシーアクションを適用します。

ステップ 6 アプライアンスは、安全な配信停止が有効になっているかどうかを確認します。安全な配信停止が有効になっている場合は、ステップ 7 に進みます。それ以外の場合は、ステップ 8 に進みます。

ステップ 7 アプライアンスは、配信停止ボタン付きのバナーをメッセージに追加します。また、アプライアンス は、メッセージ本文内の既存の配信停止リンクを書き換えます。

ステップ 8 アプライアンス は、電子メールのワークキューの次の段階でメッセージを処理します。

次のタスク

受信から配信へのルーティングまで、電子メールがシステムで処理される様子の概要については、電子メール パイプラインについてを参照してください。

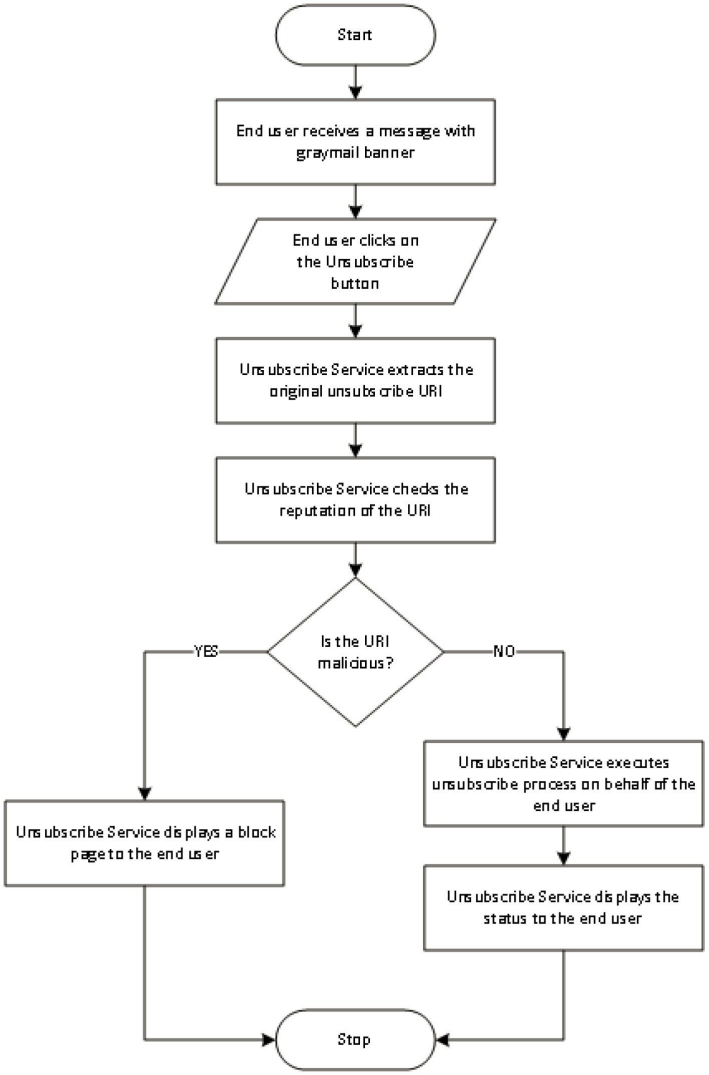
関連項目

- 安全な登録解除の仕組み （13 ページ）
- 電子メール パイプラインについて

安全な登録解除の仕組み

次のフロー チャートで、安全な配信停止のしくみを示します。

図 *2:* 安全な配信停止のワークフロー



ワークフロー（Workflow）

手順

ステップ 1 エンドユーザがグレイメール バナーを含むメッセージを受信します。

ステップ 2 エンドユーザが [購読解約（Unsubscribe）] リンクをクリックします。

ステップ 3 登録解除サービスは、元の配信停止 URI を抽出します。

ステップ 4 登録解除サービスは、URI のレピュテーションを確認します。

ステップ 5 URI のレピュテーションに応じて、登録解除サービスは次のいずれかのアクションを実行します。

- URI に悪意がある場合、登録解除サービスは配信停止プロセスを実行せず、エンドユーザにブロック ページを表示します。
- URI に悪意がない場合、URI のタイプ（http または mailto）に応じて、登録解除サービスはグレイメール送信者に配信停止要求を送信します。
  - 要求が成功した場合、登録解除サービスはエンド ユーザに [登録が解除されました（Successfully unsubscribed）] というステータスを表示します。
  - 最初の配信停止要求が失敗した場合、登録解除サービスは [配信停止プロセスの進行中（Unsubscribe process in progress）] というステータスを表示し、配信停止のステータスを追跡できる URL を示します。

    エンドユーザはこの URL を使用して後でステータスを追跡することができます。最初の試行失敗後、登録解除サービスは 4 時間の間、定期的に配信停止要求を送信します。

    エンドユーザが後から配信停止プロセスのステータスを確認した場合、次のようになります。

  - （最初の試行失敗から）4 時間以内にいずれかの要求が成功した場合、登録解除サービスはエンド ユーザに [登録が解除されました（Successfully unsubscribed）] というステータスを表示します。
  - （最初の試行失敗から）4 時間以内にいずれの要求も成功しなかった場合、登録解除サービスはエンド ユーザに [登録できません（Unable to subscribe）] というステータスを表示し、グレイメールを手動で配信停止するための URL を示します。

グレイメールの検出および安全な配信停止の設定

グレイメールの検出と安全な配信停止の要件

- グレイメールを検出するには、アンチスパム スキャンをグローバルにイネーブルにする必要があります。これにはIronPort Anti-Spam機能、インテリジェント マルチスキャン機能、またはアウトブレイク フィルタのいずれかを使用できます。「スパムおよびグレイメールの管理 （1 ページ）」を参照してください。
- 安全な配信停止の場合、
  - 安全な配信停止機能キーを追加します。
  - エンドユーザのマシンは、インターネット経由で直接クラウドベースの登録解除サービスに接続できる必要があります。

クラスタ構成でのグレイメールの検出および安全な登録解除

グレイメールの検出および安全な配信停止は、マシン レベル、グループ レベルまたはクラスタ レベルでイネーブルにできます。

グレイメールの検出および安全な配信停止の有効化

手順

ステップ 1 [セキュリティサービス（Security Services）] > [IMSおよびグレイメール（IMS and Graymail）] を選択します。

ステップ 2 [グレイメール設定（Graymail Settings）] をクリックします。

ステップ 3 [グレイメール検出を有効にする（Enable Graymail Detection）] をオンにします。

ステップ 4 [安全な配信停止を有効にする（Enable Safe Unsubscribe）] をオンにします。

ステップ 5 （任意）[自動アップデートを有効にする（Enable Automatic Updates）] をチェックして、エンジンの自動アップデートを有効にします。

アプライアンスは、アップデートサーバから特定のエンジンに必要なアップデートを取得します。

ステップ 6 **[送信（Submit）]** をクリックします。

ステップ 7 （任意）[グローバル設定の編集（Edit Global Settings）] をクリックして、メッセージ スキャンのしきい値を設定します。詳細については、Intelligent Multi-Scan とグレイメール検出のグローバル設定 （21 ページ）を参照してください。

ステップ 8 変更を送信し、保存します。

次のタスク

CLI でグレイメールの検出および安全な配信停止のグローバル設定を構成するには、`imsandgraymailconfig` の CLI コマンドを使用します。詳細については、『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

グレイメールの検出と安全な配信停止の着信メール ポリシーの設定

はじめる前に

グレイメールの検出および安全な配信停止の有効化 （15 ページ）

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] をクリックします。

ステップ 2 変更するメール ポリシーの [グレイメール（Graymail）] 列のリンクをクリックします。

ステップ 3 要件に応じて、次のオプションを選択します。

- グレイメール検出の有効化
- 安全な配信停止の有効化
- 上記のアクションをすべてのメッセージまたは未署名のメッセージのいずれに適用するかを選択します。

  （注） S/MIME を使用して暗号化されている場合または S/MIME 署名が含まれる場合、アプライアンス はメッセージを署名済みとみなします。

- さまざまなグレイメール カテゴリ（マーケティング メール、ソーシャル ネットワーク メール、およびバルク メール）に対して実行するアクション。
  - メッセージの削除、配信、バウンス、または（スパム隔離エリアへの）隔離

    （注） 安全な配信停止オプションを使用する場合、配信または隔離するアクションを設定する必要があります。

  - 代替ホストへのメッセージの送信
  - メッセージの件名の変更
  - カスタム ヘッダーの追加
  - 代替エンベロープ受信者へのメッセージの送信

    （注） グレイメール陽性メッセージを代替エンベロープ受信者に送信する場合、バナーは追加されません。

  - メッセージのアーカイブ

（注） 検出されたグレイメールのみをモニタする場合、ポリシーごとにグレイメール検出を有効にできます。さまざまなグレイメール カテゴリに対するアクションを設定する必要はありません。このシナリオでは、アプライアンスは、検出されたグレイメールに対して何もアクションを実行しません。

ステップ 4 変更を送信し、保存します。

次のタスク

（注） グレイメール検出の発信メール ポリシーを設定することもできます。このシナリオでは、安全な配信停止は設定できないことに注意してください。

CLI でグレイメールの検出および安全な配信停止用のポリシーを設定するには、**policyconfig** を使用します。詳細については、『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

グレイメール スキャン中に追加された IronPort-PHdr ヘッダー

次の場合、グレイメール エンジンによって処理されるすべてのメッセージに、IronPort PHdr ヘッダーが追加されます。

- アプライアンス でグレイメールエンジンがグローバルに有効である。
- グレイメール スキャンが特定のメール ポリシーに対して有効である。

（注） グレイメールスキャンが特定のメールポリシーに対して有効になっていない場合、アプライアンス でグレイメールエンジンがグローバルに有効であれば、すべてのメッセージに IronPort-PHdr ヘッダーが追加されます。

IronPort-PHdr ヘッダーには符号化された独自の情報が含まれており、顧客による復号はできません。このヘッダーは、グレイメールの設定に関する問題のデバッグに関する追加情報を提供します。

（注） スパム対策エンジンまたはアウトブレイク フィルタが特定のメール ポリシーに対して有効な場合、IronPort-PHdr ヘッダーは、特定のメール ポリシーを通過するすべてのメッセージに追加されます。

メッセージ フィルタを使用したグレイメール アクションのバイパス

特定のメッセージにグレイメール アクションを適用しない場合、次のメッセージ フィルタを使用してグレイメール アクションをバイパスできます。

メッセージフィルタ アクション	説明
skip-marketingcheck	マーケティング メールに対するアクションのバイパス
skip-socialcheck	ソーシャル ネットワーク メールに対するアクションのバイパス
skip-bulkcheck	バルク メールに対するアクションのバイパス

次の例では、リスナー “private_listener” で受信したメッセージは、ソーシャル ネットワーク メールに対するグレイメール アクションをバイパスする必要があること指定しています。

```
internal_mail_is_safe:
if (recv-listener == 'private_listener')
{
skip-socialcheck
();
}
```

グレイメールのモニタリング

次のレポートを使用して、検出されたグレイメールに関するデータを表示できます。

レポート	含まれるグレイメール データ	詳細
[概要（Overview）] ページ > [受信メールサマリー（Incoming Mail Summary）]	グレーメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの着信グレーメールメッセージの数と、グレーメール メッセージの総数。	[概要（Overview）] ページ

レポート	含まれるグレイメール データ	詳細
[受信メール（Incoming Mail）] ページ > [グレーメール メッセージの上位送信者（Top Senders by Graymail Messages）]	グレーメールの上位送信者。	[受信メール（Incoming Mail）] ページ
[受信メール（Incoming Mail）] ページ > [受信メールの詳細（Incoming Mail Details）]	グレーメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの着信グレーメール メッセージの数と、すべての IP アドレス、ドメイン名、またはネットワーク オーナーのグレーメール メッセージの総数。	
[受信メール（Incoming Mail）] ページ > [受信メールの詳細（Incoming Mail Details）] > [送信者プロファイル（Sender Profile）]（ドリル ダウン ビュー）	グレーメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの着信グレーメール メッセージの数と、指定された IP アドレス、ドメイン名、またはネットワーク オーナーのグレーメール メッセージの総数。	
[内部ユーザ（Internal Users）] ページ > [グレーメールの上位ユーザ（Top Users by Graymail）]	グレーメールを受信する上位エンドユーザ。	[内部ユーザ（Internal Users）] ページ
[内部ユーザ（Internal Users）] ページ > [ユーザ メール フローの詳細（User Mail Flow Details）]	グレーメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの着信グレーメール メッセージの数と、すべてのユーザのグレーメールメッセージの総数。	
[内部ユーザ（Internal Users）] ページ > [ユーザ メール フローの詳細（User Mail Flow Details）] > [内部ユーザ（Internal User）]（ドリル ダウン ビュー）	グレイメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの受信グレイメール メッセージの数と、指定されたユーザのグレイメール メッセージの総数。	

AsyncOS 9.5 以降にアップグレード後、メール ポリシーのアンチスパム設定でマーケティング メールのスキャンをイネーブルにした場合は、次の点に注意してください。

- マーケティング メッセージの数は、アップグレードの前後に検出されたマーケティング メッセージの合計です。
- グレイメール メッセージの総数には、アップグレードの前に検出されたマーケティング メッセージの数は含まれません。
- 試行されたメッセージの総数には、アップグレードの前に検出されたマーケティング メッセージの数も含まれます。

グレイメール ルールの更新

サービスのアップデートをイネーブルにした場合、シスコのアップデート サーバからグレイメール管理ソリューションのスキャン ルールを取得できます。しかし、一部のシナリオでは（たとえば、サービスの自動アップデートをディセーブルにした場合またはサービスの自動アップデートが機能していない場合）、グレイメール ルールを手動で更新できます。

グレイメール ルールを手動で更新するには、次のいずれかを実行します。

- Web インターフェイスで、[セキュリティサービス（Security Services）] > [IMSおよびグレイメール（IMS and Graymail）] ページに移動して [今すぐ更新（Update Now）] をクリックします。
- CLI で graymailupdate コマンドを実行します。

既存のグレイメール ルールの詳細を確認するには、Web インターフェイスで [IMSおよびグレイメール（IMS and Graymail）] ページの [ルールの更新（Rule Updates）] を確認するか、または CLI で graymailstatus コマンドを使用します。

エンドユーザに表示される [登録解除（Unsubscribe）] ページのカスタマイズ

エンドユーザが配信停止リンクをクリックすると、登録解除サービスにより、配信停止プロセスのステータスを示すシスコブランドの配信停止ページが表示されます（安全な登録解除の仕組み （13 ページ）を参照）。[セキュリティ サービス（Security Services）] > [ブロック ページ カスタマイズ（Block Page Customization）] を使用して、配信停止ページの外観および組織のブランディングの表示（企業ロゴ、連絡先情報など）をカスタマイズできます。この説明については、サイトに悪意がある場合にエンド ユーザに表示する通知のカスタマイズ を参照してください。

エンドユーザのセーフリスト

組織のエンド ユーザが自分の電子メール アカウントのセーフリストを設定している場合は、セーフリストの送信者からのグレイメール メッセージはグレイメール スキャン エンジンによってスキャンされません。セーフリストの詳細については、セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御を参照してください。

ログの表示

グレイメールの検出および安全な配信停止情報は、次のログに書き込まれます。

- **グレイメール エンジン ログ**。グレイメール エンジン、ステータス、設定などの情報が含まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。
- **グレイメール アーカイブ**。アーカイブされたメッセージ（スキャン済みの「アーカイブ メッセージ」アクションに関連付けられているメッセージ）が含まれます。この形式は、mbox 形式のログ ファイルです。
- **メール ログ**。グレイメールの検出および安全な配信停止用のバナーの追加についての情報が含まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

グレイメールの検出および安全な配信停止のトラブルシューティング

安全な配信停止を実行できない （21 ページ）

安全な配信停止を実行できない

問題

配信停止リンクをクリックした後、エンドユーザに「...を配信停止できません」というメッセージが表示されます。

解決方法

この問題は、登録解除サービスがエンドユーザの代わりに安全な配信停止を実行できない場合に発生することがあります。次に、登録解除サービスが安全な配信停止を実行できない一般的なシナリオをいくつか示します。

- 配信停止 URI または mailto アドレスが間違っている。
- 配信停止にエンドユーザのクレデンシャルを要求する Web サイト。
- エンドユーザに自分の電子メール アカウントにログインし、配信停止要求を確認するように要求する Web サイト。
- Web サイトで captcha を解決するよう要求され、登録解除サービスで captcha を解決できない。
- インタラクティブな配信停止を必要とする Web サイト。

エンドユーザは [購読解約（Unsubscribe）] ページの下部に表示されている URL を使用して購読解約を手動で行えます。

Intelligent Multi-Scan とグレイメール検出のグローバル設定

アプライアンス のスループットを最適化するために、Cisco Intelligent Multi-Scan とグレイメールによってメッセージをスキャンするしきい値とタイムアウトを設定できます。これらの設定は、Cisco Intelligent Multi-Scan とグレイメールの設定に共通です。

1. [セキュリティサービス（Security Services）] > [IMSおよびグレイメール（IMS and Graymail）] を選択します。
2. [グローバル設定を編集（Edit Global Settings）] をクリックします。
3. Cisco Intelligent Multi-Scan とグレイメール検出でスキャンするしきい値を選択します。

   デフォルトの値は次のとおりです。

   - 512 K 以下は常にスキャンします。
   - 

     （注） この設定は、グレイメール検出と安全な配信停止には適用されません。
   - 1 M 超はスキャンしないでください。
4. 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。

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。最大メッセージサイズの設定を小さくして、アプライアンス のスループットを最適化できる可能性があります。

5. 変更を送信して確定します。

スパム対策ポリシーの定義

各メールポリシーで、スパムと見なされるメッセージと、これらのメッセージで行われるアクションを指定します。また、ポリシーが適されるメッセージをスキャンするエンジンを指定します。

デフォルトの着信および発信メールポリシーに対して、異なる設定を設定できます。別のユーザに異なるスパム対策ポリシーが必要な場合は、異なるスパム対策設定を持つ複数のメールポリシーを使用します。ポリシーごとに1つのスパム対策ソリューションだけをイネーブルにできます。同じポリシーに両方をイネーブルにすることはできません。

はじめる前に

- メッセージがスパムかどうかスキャンするためのアプライアンス の設定方法 （2 ページ）のテーブルの、ここまでのすべてのステップを実行します。
- 次の概念を十分に理解してください。
  - 陽性および陽性と疑わしいスパムのしきい値について （25 ページ）
  - 設定例：陽性と判定されたスパムに対するアクションと陽性と疑わしいスパムに対するアクション （26 ページ）
  - 正規の送信元からの不要なマーケティング メッセージ （26 ページ）
  - 複数のスパム対策ソリューションをイネーブルにした場合：異なるメールポリシーでの異なるスパム対策スキャン エンジンの有効化：設定例 （28 ページ）
  - スパム対策スキャン中に追加されるヘッダー （30 ページ）
- 「スパム対策アーカイブ」ログにスパムをアーカイブする場合は、ログも参照してください。
- 代替メールホストにメッセージを送信する場合は、配信ホスト変更アクションも参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] ページに移動します。

または

ステップ 2 [メールポリシー（Mail Policies）] > [発信メールポリシー（Outgoing Mail Policies）] ページに移動します。

ステップ 3 [スパム対策（Anti-Spam）] 列で、任意のメール ポリシーのリンクをクリックします。

ステップ 4 [このポリシーのスパム対策スキャンを有効にする（Enable Anti-Spam Scanning for this Policy）] セクションでは、ユーザがポリシーで使用するスパム対策ソリューションを選択します。

表示されるオプションは、イネーブルにしたスパム対策スキャン ソリューションに基づきます。

デフォルト以外のメールポリシーの場合、デフォルトのポリシーを使用すると、そのページの他のオプションはディセーブルになります。

このメールポリシーに対してスパム対策スキャンをまとめてディセーブルにすることもできます。

ステップ 5 スパムであることが確実な電子メール、スパムだと疑われる電子メール、およびマーケティング メッセージの設定を行います。

オプション	説明
スパムだと疑われる電子メールのスキャンを有効にする（Enable Suspected Spam Scanning） マーケティング電子メールのスキャンを有効にする（Enable Marketing Email Scanning）	オプションを選択します。 陽性と判定されたスパムのスキャンはスパム対策スキャンが有効の場合は常に有効です。
このアクションをメッセージに適用する（Apply This Action to Message）	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選択します。 • デリバリ • ドロップ（Drop） • バウンス（Bounce） • 検疫（Quarantine）
（任意）代替ホストに送信（Send to Alternate Host）	識別されたメッセージを別の宛先メールホスト（SMTP ルートまたは DNS に示されているもの以外のメール サーバ）に送信できます。 IP アドレスまたはホスト名を入力します。ホスト名を入力すると、Mail Exchange（MX）が最初に検索されます。キーが見つからない場合、DNS サーバの A レコードが使用されます（SMTP ルートと同じ）。 たとえば、追加の検査のサンドボックスのメールサーバなど、メッセージの方向を変更するにはこのオプションを使用します。 重要な詳細情報については、配信ホスト変更アクションを参照してください。

オプション	説明
件名へテキストを追加（Add Text to Subject）	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できます。 （注） この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）。たとえば付加した場合、少数の末尾にスペースを含むテキスト [SPAM] を追加します。 [件名へテキストを追加（Add Text to Subject）] フィールドでは US-ASCII 文字だけが許可されます。
[詳細オプション（Advanced Options）]（カスタム ヘッダーとメッセージ配信用）	
カスタムヘッダーを追加(オプション)（Add Custom Header (Optional)）	識別されたメッセージにカスタム ヘッダーを追加できます。 [詳細（Advanced）] をクリックし、ヘッダーと値を定義します。 カスタム ヘッダーとコンテンツ フィルタを併用することで、陽性と疑わしいスパム メッセージ内の URL をリダイレクトして Cisco Web セキュリティ プロキシ サービスにパススルーするなどのアクションを実行できます。詳細については、カスタムヘッダーを使用して、陽性と疑わしいスパム内の URL を Cisco Web セキュリティ プロキシにリダイレクトする：設定例 （27 ページ）を参照してください。
（任意）代替エンベロープ受信者に送信（Send to an Alternate Envelope Recipient）	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。 [詳細（Advanced）] をクリックして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。
アーカイブ メッセージ（Archive Message）	識別されたメッセージを「スパム対策アーカイブ」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。
スパムしきい値（Spam Thresholds）	デフォルトのしきい値を使用するか、陽性と判定されたスパムのしきい値および陽性と疑わしいスパムの値を入力します。

ステップ 6 変更を送信し、保存します。

次のタスク

発信メールのスパム対策スキャンをイネーブルにした場合は、特にプライベートリスナーに関連するホストアクセステーブルのスパム対策設定を確認します。メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義を参照してください。

関連項目

- メッセージがスパムかどうかスキャンするためのアプライアンス の設定方法 （2 ページ）
- 陽性および陽性と疑わしいスパムのしきい値について （25 ページ）
- 設定例：陽性と判定されたスパムに対するアクションと陽性と疑わしいスパムに対するアクション （26 ページ）
- 正規の送信元からの不要なマーケティング メッセージ （26 ページ）
- カスタム ヘッダーを使用して、陽性と疑わしいスパム内の URL を Cisco Web セキュリティ プロキシにリダイレクトする：設定例 （27 ページ）
- 異なるメール ポリシーでの異なるスパム対策スキャン エンジンの有効化：設定例 （28 ページ）

陽性および陽性と疑わしいスパムのしきい値について

メッセージがスパムであるかどうかを評価するときに、両方のスパム対策スキャン ソリューションは、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。スコアは、メッセージをスパムとして見なすかどうかを決定するため、該当するメールポリシーで指定されたしきい値と比較されます。

最高精度では、スパムとして陽性と識別する精度はデフォルトでかなり高く設定されています。90～100 の範囲のメッセージ スコアは、陽性と判定されたスパムであると見なされます。陽性と疑わしいスパムのデフォルトのしきい値は 50 です。

- 陽性と疑わしいスパムのしきい値未満のスコアを持つメッセージは正規のメッセージと見なされます。
- 陽性と疑わしいスパムのしきい値を超えているが、陽性と識別されたしきい値未満のメッセージは、スパムの疑いがあると見なされます。

各メールポリシーで陽性および陽性と疑わしいスパムのしきい値をカスタマイズし、組織のスパムの許容レベルを反映するスパム対策ソリューションを設定できます。

50～99 の値に陽性と判定されたスパムのしきい値を変更できます。25 から陽性と判定されたスパムに指定した値までの範囲の任意の値に、陽性と疑わしいスパムのしきい値を変更できます。

しきい値を変更する場合：

- 低い番号（より積極的な設定）を指定すると、より多くのメッセージをスパムとして識別し、より多くの誤検出が生成される場合があります。これによって、ユーザがスパムを受けるリスクは低くなりますが、スパムとしてマークされた正規のメールを受けるリスクは高くなります。

- より高い数（より保守的な設定）を指定すると、より少ないメッセージをスパムとして識別し、より多くのスパムを配信する可能性があります。これによって、ユーザがスパムを受けるリスクは高くなりますが、正規のメールがスパムとして除かれるリスクは低くなります。理想的には、正しく設定した場合、メッセージの件名はそのメッセージがスパムである可能性が高いことを識別し、メッセージは配信されます。

陽性と判定されたスパムと陽性と疑わしいスパムに対して異なるアクションを定義できます。たとえば、「陽性と判定された」スパムをドロップしますが、「陽性と疑わしい」スパムは隔離します。

関連項目

- スパム対策ソリューション　（2 ページ）
- 設定例：陽性と判定されたスパムに対するアクションと陽性と疑わしいスパムに対するアクション　（26 ページ）

設定例：陽性と判定されたスパムに対するアクションと陽性と疑わしいスパムに対するアクション

スパム	サンプル アクション（**Aggressive**）	サンプル アクション（**Conservative**）
陽性と判定された	削除	• メッセージの件名に「`[Positive Spam]`」を追加して配信、または • 検疫（Quarantine）
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

積極的な例では、陽性と識別されたメッセージをドロップし、スパムの疑いのあるメッセージだけにタグを付けます。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、誤検出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。

保守的な例では、陽性と判定されたスパムと陽性と疑わしいスパムは、件名を変更して通過されます。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 番目の方式よりも保守的です。

メール ポリシーの積極的および保守的なポリシーの詳細については、管理例外を参照してください。

正規の送信元からの不要なマーケティング メッセージ

マーケティング電子メール設定をメール ポリシーのアンチスパム設定の下に構成した場合、AsyncOS 9.5 for Email へのアップグレード後、アンチスパム設定の下のマーケティング電子メー

ル設定は同じポリシーのグレイメール設定の下に移動されます。スパムおよびグレイメールの管理 （1 ページ） を参照してください。

カスタムヘッダーを使用して、陽性と疑わしいスパム内のURLをCisco Web セキュリティ プロキシにリダイレクトする：設定例

受信者が陽性と疑わしいスパム内のリンクをクリックしたときに、その要求が Cisco Web セキュリティ プロキシ サービスにルーティングされるように、メッセージ内の URL を書き換えることができます。これにより、クリック時にサイトの安全性が評価され、既知の悪意のあるサイトへのアクセスがブロックされます。

はじめる前に

URL フィルタリング機能とその前提条件をイネーブルにしてください。URL フィルタリングの設定を参照してください。

手順

ステップ 1 陽性と疑わしいスパム メッセージにカスタム ヘッダーを適用します。

a) [メールポリシー（Mail Policies）]>[受信メールポリシー（Incoming Mail Policies）] を選択します。
b) [スパム対策（Anti-Spam）]列で、ポリシー（デフォルト ポリシーなど）のリンクをクリックします。
c) [サスペクトスパムの設定（Suspected Spam Settings）] セクションで、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。
d) [詳細（Advanced）] をクリックして、[カスタムヘッダーを追加（Add Custom Header）] オプションを表示します。
e) url_redirect などのカスタム ヘッダーを追加します。
f) 変更を送信し、保存します。

ステップ 2 カスタム ヘッダーを持つメッセージ内の URL をリダイレクトするコンテンツ フィルタを作成します。

a) [メールポリシー（Mail Policies）]>[受信コンテンツフィルタ（Incoming Content Filters）] を選択します。
b) [フィルタの追加（Add Filter）] をクリックします。
c) フィルタに url_redirect という名前を付けます。
d) [条件を追加（Add Condition）] をクリックします。
e) [その他のヘッダー（Other Header）] をクリックします。
f) ヘッダー名 url_redirect を入力します。

これが上記で作成したヘッダーと正確に一致することを確認してください。

g) [ヘッダーが存在（Header exists）] を選択します。
h) [OK] をクリックします。

i) [アクションを追加（Add Action）] をクリックします。
j) [URLカテゴリ（URL Category）] をクリックします。
k) [利用可能なカテゴリ（Available Categories）] ですべてのカテゴリを選択し、[選択したカテゴリ（Selected Categories）] に追加します。
l) [URLに対するアクション（Action on URL）] で、[Cisco Security Proxyにリダイレクト（Redirect to Cisco Security Proxy）] を選択します。
m) [OK] をクリックします。

ステップ 3 メール ポリシーにコンテンツ フィルタを追加します。

a) [メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] を選択します。
b) [コンテンツフィルタ（Content Filters）] 列で、前の手順で選択したポリシーのリンクをクリックします。
a) [コンテンツフィルタを有効にする（Enable Content Filters）] を選択します（選択されていない場合）。
b) チェックボックスを選択して、**url_filtering** コンテンツ フィルタをイネーブルにします。
c) 変更を送信し、保存します。

次のタスク

関連項目

- URL のリダイレクト
- コンテンツ フィルタ

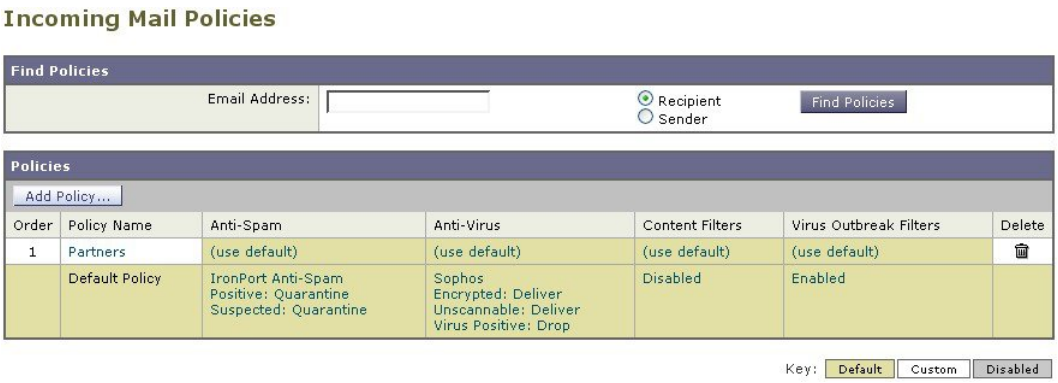
異なるメール ポリシーでの異なるスパム対策スキャン エンジンの有効化：設定例

システム セットアップ ウィザード（またはCLI の systemsetup コマンド）を使用すると、Cisco Intelligent Multi-Scan または Cisco 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中に両方をイネーブルにできませんが、システムセットアップが完了した後に[セキュリティサービス（Security Services）]メニューを使用して、選択しなかったスパム対策ソリューションをイネーブルにできます。

システムのセットアップが終了すれば、[メール ポリシー（Mail Policies）] > [着信メール ポリシー（Incoming Mail Policies）] ページから着信メール ポリシー用のスパム対策スキャン ソリューションを設定できます（スパム対策スキャンは、発信メール ポリシーでは通常無効です）。ポリシーのスパム対策スキャンもディセーブルにできます。

この例では、デフォルトのメールポリシーおよび「パートナー」ポリシーで、陽性スパムおよび陽性と疑わしいスパムを隔離するために Cisco Anti-Spam スキャン エンジンを使用しています。

図 *3 :* メール ポリシー：受信者ごとのスパム対策エンジン

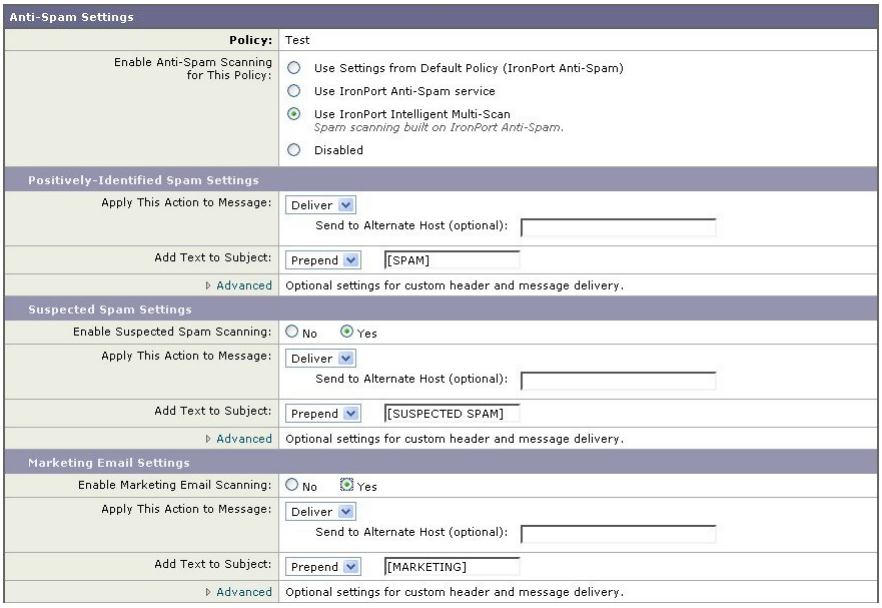


パートナーのポリシーを変更して、不要なマーケティング メッセージに対して Cisco Intelligent Multi-Scan とスキャンを使用するには、パートナーの行に対応する [スパム対策（Anti-Spam）] 列のエントリ（[デフォルトを使用（Use Default）]）をクリックします。

スキャン エンジンに Cisco Intelligent Multi-Scan を選択し、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する場合は [はい（Yes）] を選択します。不要なマーケティング メッセージの検出にデフォルト設定を使用します。

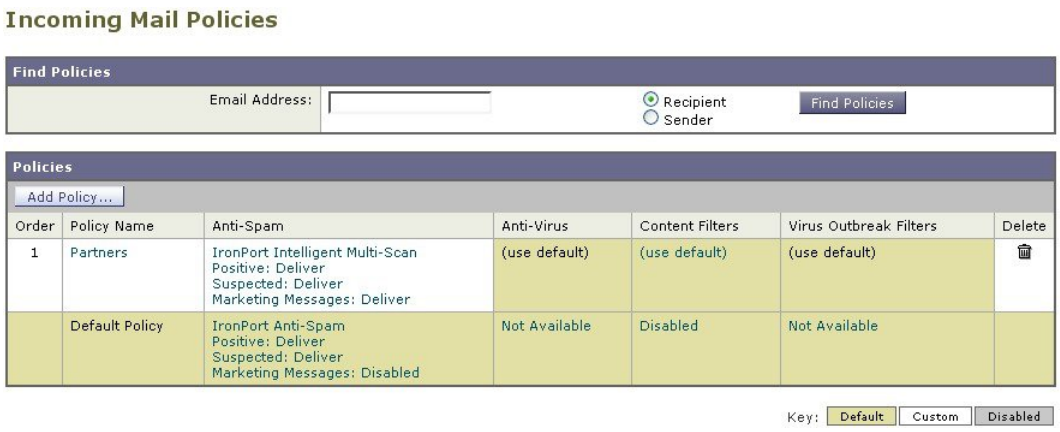
次の図は、Cisco Intelligent Multi-Scan と不要なマーケティング メッセージの検出がポリシーでイネーブルに設定されていることを示します。

図 *4 :* メール ポリシー：*Cisco Intelligent Multi-Scan* のイネーブル化



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



スパムフィルタからのアプライアンス生成メッセージの保護

アプライアンスから自動送信された電子メールメッセージ（メールアラートおよびスケジュールレポートなど）には、誤ってスパムとして識別される可能性のある URL または他の情報が含まれることがあるため、確実に配信されるよう次を実行します。

スパム対策スキャンをバイパスする着信メールポリシーにこれらのメッセージの送信者を含めます。送信者および受信者のグループのメール ポリシーの作成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。

スパム対策スキャン中に追加されるヘッダー

- いずれかのスパム対策スキャン エンジンがメール ポリシーでイネーブルにされている場合、そのポリシーを通過した各メッセージは次のヘッダーをメッセージに追加します。

  X-IronPort-Anti-Spam-Filtered: true

  X-IronPort-Anti-Spam-Result

  2 番目のヘッダーには、メッセージのスキャンに使用されたルールとエンジンのバージョンをシスコ サポートで識別するための情報が含まれます。結果の情報は、符号化された独自の情報であり、顧客による復号は可能ではありません。

- Cisco 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。
- 陽性と判定されたスパム、陽性と疑わしいスパム、不要なマーケティング メールとして識別される特定のメールポリシーのすべてのメッセージに追加する追加のカスタムヘッダーを定義できます。スパム対策ポリシーの定義　（22 ページ）を参照してください。

関連項目

- カスタム ヘッダーを使用して、陽性と疑わしいスパム内の URL を Cisco Web セキュリティ プロキシにリダイレクトする：設定例 （27 ページ）

誤って分類されたメッセージのシスコへの報告

分類が誤っていると思われるメッセージを、分析用にシスコに報告できます。報告されたメッセージは、製品の精度および有効性を高めるために使用されます。

誤って分類されたメッセージは、次のカテゴリに属するものを報告いただけます。

- 検出されなかったスパム
- スパムとしてマークされたがスパムではないメッセージ
- 検出されなかったマーケティング メッセージ
- マーケティング メッセージとしてマークされたがマーケティング メッセージではないメッセージ
- 検出されなかったフィッシング メッセージ

関連項目

- 誤って分類されたメッセージのシスコへの報告方法 （31 ページ）
- 送信を追跡する方法 （37 ページ）

誤って分類されたメッセージのシスコへの報告方法

はじめる前に

誤って分類されたメッセージをシスコに報告する前に、次の手順を実行する必要があります。この手順は一度だけ実行してください。

手順

ステップ 1 Cisco Talos 電子メールステータスポータルで管理者として登録するには、次のいずれかの方法を使用します。

（注） Cisco Talos 電子メールステータスポータルは、電子メール管理者がポータル上で電子メール送信を表示および追跡できる Web ベースのツールです。

- 組織内で初めてポータルにアクセスする管理者である場合の登録：

  1. シスコのクレデンシャルを使用して Cisco Talos 電子メールステータスポータル（https://talosintelligence.com/email_status_portal）にログインします。
  2. [アカウントの管理（Manage Account）] をクリックします。
  3. [ドメインの追加（Add Domain）] をクリックします。

4. ドメインをポータルに登録するには、[ドメイン（Domain）]フィールドに組織のドメイン名を入力します。

   （注） 必ず有効なドメイン名を入力します。たとえば、`example.com` は電子メールアドレス `user@example.com` のドメイン名です。組織内に複数のドメインがある場合は、必ずすべてのドメインを追加します。

5. ステップ「d」で入力したドメインの所有者である場合は、[所有するドメイン（I own this domain）] チェックボックスをオンにします。

   （注） [所有するドメイン（I own this domain）] チェックボックスをオンにしない場合、ドメインの表示アクセス権のみが付与されます。詳細については、次の URL にある Cisco Talos 電子メールステータスポータルのヘルプページを参照してください。 https://talosintelligence.com/tickets/email_submissions/help

6. **[送信（Submit）]** をクリックします。

   [送信（Submit）] をクリックすると、6 桁の文字の確認コードを示す電子メールが自動的に `postmaster@domain.com`（domain.com はステップ「d」で入力したドメイン）に送信され、ドメインの所有権が確認されます。

   組織が `postmaster@domain.com` を使用していないか、または管理者に postmaster メールボックスへのアクセス権がない場合には、メッセージフィルタを（すべてのアプライアンス上で）作成して、`SubmissionPortal@cisco.com` から `postmaster@domain.com` に送信されるメッセージを別の電子メールアドレスにリダイレクトします。次に示すのは、サンプルのメッセージ フィルタです。

   ```
   redirect_postmaster: if (rcpt-to == "postmaster@domain.com") AND (mail-from ==
   "^SubmissionPortal@cisco.com$") { alt-rcpt-to ("admin@domain.com"); }
   ```

7. [ドメイン所有者確認コード（Domain Ownership Verification Code）] ダイアログボックスに 6 桁の文字の確認コードを入力して、ドメインの所有権を確認します。
8. [確認コードの送信（Submit Verification Code）] をクリックします。

   [確認コードの送信（Submit Verification Code）] ボタンをクリックすると、自動的に管理者アクセス権が付与されます。登録 ID が自動的に生成され、ポータルの [アカウントの管理（Manage Accounts）] セクションで確認できます。この登録 ID は組織内すべてのアプライアンスで使用できます。

   （注） 登録 ID は、特定の組織に属している Cisco E メールセキュリティ ゲートウェイから行われた送信を識別するための一意の ID です。

- 組織内の管理者がポータルにすでに登録されている場合の登録：

1. シスコのクレデンシャルを使用して Cisco Talos 電子メールステータスポータル（https://talosintelligence.com/email_status_portal）にログインします。
2. [アカウントの管理（Manage Account）] をクリックします。
3. [ドメインの追加（Add Domain）] をクリックします。

4. ドメインをポータルに登録するには、[ドメイン（Domain）]フィールドに組織のドメイン名を入力します。

   （注） 必ず有効なドメイン名を入力します。たとえば、`example.com` は電子メールアドレス `user@example.com` のドメイン名です。組織内に複数のドメインがある場合は、必ずすべてのドメインを追加します。

5. **[送信（Submit）]** をクリックします。

[登録（Register）]をクリックすると、すでにポータルに登録されている管理者に電子メール通知が送信されます。この管理者はポータルにログインし、[アカウントの管理（Manage Accounts）] の [権限要求（Permission Requests）] セクションで [承認（Approve）] をクリックして、登録要求を承認する必要があります。

登録要求が承認されると、登録IDが自動的に生成され、ポータルの[アカウントの管理（Manage Accounts）]セクションに表示できます。この登録 ID は組織内すべてのアプライアンスで使用できます。

（注） 登録 ID は、特定の組織に属している Cisco E メール セキュリティ ゲートウェイから行われた送信を識別するための一意の ID です。

ステップ 2 組織内のすべてのアプライアンスについて、Cisco Talos 電子メールステータスポータルから生成された登録 ID を追加します。

1. Web インターフェイスを使用してアプライアンス にログインします。
2. [システム管理（System Administration）] > [Cisco Talos 電子メールステータスポータル登録（Cisco Talos Email Status Portal Registration）] に移動します。
3. アプライアンスがクラスタの一部である場合は、モードをクラスタレベルに設定します。
4. [登録 ID の設定（Set Registration ID）] をクリックします。
5. [登録ID（Registration ID）]フィールドに、Cisco Talos 電子メールステータスポータルから取得した登録 ID を入力します。
6. 変更を送信し、保存します。
7. アプライアンスがクラスタの一部ではない場合、組織内すべてのアプライアンスでステップ 1 ～ 6 を繰り返す必要があります。

CLI で `portalregistrationconfig` コマンドを使用して登録 ID を設定することもできます。

誤って分類されたメッセージのシスコへの報告方法

詳細については、以下を参照してください。

- 『How to Submit Email Messages to Cisco』ドキュメント（https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214133-how-to-submit-email-messages-to-cisco.html#anc5）。

- Cisco Talos 電子メールステータスポータルのヘルプページ（https://talosintelligence.com/tickets/email_submissions/help）。

手順

ステップ 1 誤って分類されたメッセージのシスコへの報告方法 （31 ページ）の「**はじめる前に**」の項に記載されている手順を実行します。

ステップ 2 誤って分類されたメッセージをシスコに報告するには、次の方法のいずれかを使用します。

- Cisco E メール セキュリティ プラグインの使用 （34 ページ）
- 誤って分類されたメッセージの添付ファイルとしての転送 （35 ページ）

誤って分類されたメッセージをシスコに報告すると、ポータルの [アカウントの管理（Manage Account）] セクションにある [電子メール通知とレポート（Email Notification and Reports）] ボタンで選択したオプションに基づいた電子メール通知を受信します。

（注） [電子メール通知とレポート（Email Notification and Reports）] ボタンの下にある [マイ送信通知（My Submission Notifications）] および [マイ送信レポート（My Submission Reports）] オプションは、デフォルトでオフに設定されています。詳細については、次の URL にある Cisco Talos 電子メールステータスポータルのヘルプページを参照してください。 https://talosintelligence.com/tickets/email_submissions/help

次のタスク

送信を追跡する方法 （37 ページ）

Cisco E メール セキュリティ プラグインの使用

Cisco Email Security Plug-In は、Microsoft Outlook を使用してユーザ（電子メール管理者とエンドユーザ）が誤って分類されたメッセージをシスコへ報告できるようにするツールです。このプラグインを Microsoft Outlook の一部として展開する場合、レポート メニューが Microsoft Outlook の Web インターフェイスに追加されます。このプラグインのメニューを使用して、誤って分類されたメッセージをレポートできます。

その他の情報

- 次のページから Cisco Email Security Plug-In をダウンロードできます：https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=284900944&flowid=41782&softwareid=283090986。
- 詳細については、『Cisco Email Security Plug-In Administrator Guide』http://www.cisco.com/c/en/us/support/security/email-encryption/products-user-guide-list.htmlを参照してください。

誤って分類されたメッセージの添付ファイルとしての転送

メッセージのカテゴリに応じて、以下の表に表示されているアドレスにRFC 822添付ファイルとしてそれぞれの誤って分類されたメッセージを転送できます。

電子メールの送信	定義	送信方法	送信に関するユーザの考慮事項
スパム/フィッシング	未承認および望ましくないメール。スパム/フィッシングは正当ではなく、悪意のあるもの（フィッシング、ウイルス、マルウェア、詐欺など）である可能性もあります。	spam@access。 ironport.com phish@access。 ironport.com virus@access。 ironport.com Outlookプラグインの[迷惑メール（Spam）]、[フィッシング（Phish）]、または[ウイルス（Virus）]ボタン	ユーザの受信トレイに配信されますが、ユーザはメッセージをスパムまたはフィッシングと見なします。 スパムとして検出されましたが、ユーザは正当なメッセージと見なします。
正当 mate	スパムではなく、正当な（正常な）電子メール。「ハム」とも呼ばれます。	ham@access。 ironport.com Outlookプラグインの[迷惑メールではない（Not Spam）]ボタン	マーケティング/グレイメールメッセージはマーケティング/グレイメールとして検出されない。

電子メールの送信	定義	送信方法	送信に関するユーザの考慮事項
マーケティング/グレイメール	マーケティングは、商用のバルク電子メールである正当な（スパムではない）電子メールです。通常はサブスクリプションベースで、不要な場合もあります。 ユーザは、送信者に対し故意または無意識にメールを要求した可能性があります。たとえば、会議でバッジをスワイプしたり、オンラインで購入した場合が考えられます。正当なサブスクリプションベースのマーケティング電子メールには、購読解除メカニズムがあります。 グレイメールは、マーケティングおよびその他の正当なバルク電子メールを含むより広範囲なカテゴリです。	ads@access。 ironport.com Outlook プラグインの[マーケティング（Marketing）] ボタン	スパムとして検出されても、ユーザは正当なメッセージと見なします。
非マーケティング/グレイメール	バルクでもサブスクリプションベースでもない正規の電子メール（スパムではない）。通常、個人間や取引に関するものです。	not_ads@access。 ironport.com	マーケティング/グレイメールとしてとして検出されても、ユーザはメッセージを取引関連またはマーケティング/グレイメールではないものと見なします。

次の電子メールプログラムのいずれかを使用してメッセージを転送すると、最適な結果を得ることができます。

- Apple Mail
- Microsoft Outlook for Mac
- Microsoft Outlook Web App
- Mozilla Thunderbird

注意 Microsoft Outlook 2010、2013、2016 for Microsoft Windows を使用している場合は、誤って分類されたメッセージを報告するのに、Cisco Email Security Plug-In または Microsoft Outlook Web App を使用する必要があります。これは、Windows 用の Outlook が必要なヘッダーをそのままにしてメッセージを転送できないためです。また、添付ファイルとして元のメッセージを転送することができる場合にのみ、モバイル プラットフォームを使用します。

送信を追跡する方法

送信の詳細が示された電子メール通知を受け取ったら、Cisco Talos 電子メールステータスポータルで送信を表示および追跡できます。

手順

ステップ 1 シスコのクレデンシャルを使用して Cisco Talos 電子メールステータスポータル（https://talosintelligence.com/email_status_portal）にログインします。

ステップ 2 Cisco Talos 電子メールステータスポータルで [送信（Submissions）] をクリックします。

ステップ 3 [フィルタオプション（Filter Options）] をクリックし、適切なフィルタオプションを選択します。

ステップ 4 （オプション）カレンダーボタンをクリックして、特定の日付を選択します。

次のタスク

詳細については、Cisco Talos 電子メールステータスポータルのヘルプページ（https://talosintelligence.com/tickets/email_submissions/help）を参照してください。

着信リレー構成における送信者の IP アドレスの決定

1 つ以上のメール交換/転送エージェント（MX または MTA）、フィルタサービスなどがアプライアンスと着信メールを送信する外部マシンとの間のネットワークのエッジに配置されている場合、アプライアンス は送信元マシンの IP アドレスを決定することはできません。代わりに、メールはローカル MX/MTA から送信されたように見えます。ただし、IronPort Anti-Spam および Cisco Intelligent Multi-Scan（IP レピュテーションサービスを使用）は外部送信者の正確な IP アドレスに依存します。

ソリューションは、着信リレーを使用するようにアプライアンスを設定することです。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、発信元 IP アドレスを保管するのに使用するヘッダーを指定します。

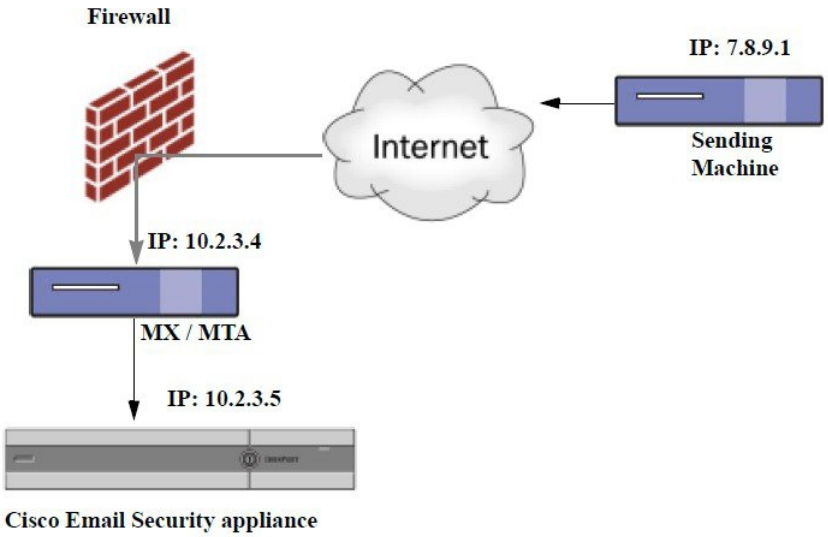
関連項目

- 着信リレーを使用した環境例 （38 ページ）
- 着信リレーを使用するアプライアンス の設定 （39 ページ）
- 着信リレーが機能にどのように影響するか （45 ページ）
- 使用するヘッダーを指定するログの設定 （47 ページ）

着信リレーを使用した環境例

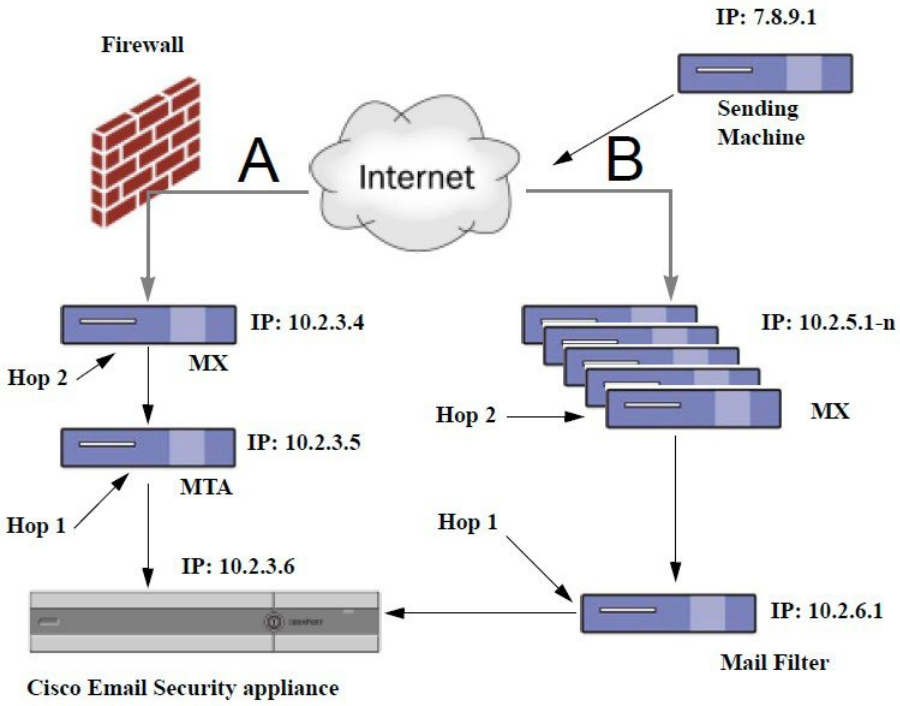
次の図に、着信リレーの非常に基本的な例を示します。ローカル MX/MTA によってメールがアプライアンス にリレーされているため、IP アドレス 7.8.9.1 からのメールは IP アドレス 10.2.3.4 からのように見えます。

図 *6 : MX/MTA* によるメール リレー：簡易



次の図に別の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、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、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、アプライアンス に配信されます。

図 *7 : MX/MTA* によるメール リレー：拡張



着信リレーを使用するアプライアンス の設定

関連項目

- 着信リレー機能のイネーブル化　（39 ページ）
- 着信リレーの追加　（40 ページ）
- リレーされたメッセージのメッセージ ヘッダー　（41 ページ）

着信リレー機能のイネーブル化

（注）　ローカル MX/MTA がメールをアプライアンス にリレーする場合のみ、着信リレー機能をイネーブルにしてください。

手順

ステップ 1　[ネットワーク（Network）] > [着信リレー（Incoming Relays）] を選択します。

ステップ 2　**[有効（Enable）]** をクリックします。

ステップ 3 変更を保存します。

着信リレーの追加

識別する着信リレーを追加します。

- アプライアンス に着信メッセージをリレーするネットワークの各マシン、および
- 元の外部送信者の IP アドレスが分類されるヘッダー。

はじめる前に

これらの前提条件を完了するために必要な情報は、リレーされたメッセージのメッセージヘッダー （41 ページ）を参照してください。

- 元の外部送信者の IP アドレスを識別するカスタムまたは Received ヘッダーを使用するかどうかを設定します。
- カスタム ヘッダーを使用する場合：
  - リレーされたメッセージの発信元 IP アドレスを分類する正確なヘッダーを設定します。
  - 各 MX、MTA、または元の外部送信元に接続している他のマシンは、受信メッセージに元の外部送信者のヘッダー名と IP アドレスを追加するには、そのマシンを設定します。

手順

ステップ 1 [ネットワーク（Network）] > [着信リレー（Incoming Relays）] を選択します。

ステップ 2 [リレーの追加（Add Relay）] をクリックします。

ステップ 3 このリレーの名前を入力します。

ステップ 4 MTA、MX、または着信メッセージをリレーするためにアプライアンスに接続している他のマシンの IP アドレスを入力します。

IPv4 または IPv6 アドレス、標準 CIDR 形式、または IP アドレス範囲を使用できます。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。

IPv6 アドレスの場合、AsyncOS は次の形式をサポートします。

- `2620:101:2004:4202::0-2620:101:2004:4202::ff`
- `2620:101:2004:4202::`
- `2620:101:2004:4202::23`
- `2620:101:2004:4202::/64`

ステップ 5 元の外部送信者の IP アドレスを識別するヘッダーを指定します。

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。

a) ヘッダー タイプの選択：

カスタム ヘッダー（推奨）または Received ヘッダーを選択します。

b) カスタム ヘッダーの場合：

リレーされたメッセージに追加するリレー マシンを設定したヘッダー名を入力します。

次に例を示します。

```
SenderIP
```

または

```
X-CustomHeader
```

c) Received ヘッダーの場合：

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。

ステップ 6 変更を送信し、保存します。

次のタスク

次を行うことを検討します。

- DHAP の無制限のメッセージがあるメール フロー ポリシーを送信者グループにリレーするマシンを追加します。説明については、着信リレーおよびディレクトリ ハーベスト攻撃防止 （45 ページ）を参照してください。
- トラッキングおよびトラブルシューティングを容易にするには、使用されるヘッダーを示すようにアプライアンスのロギングを設定します。使用するヘッダーを指定するログの設定 （47 ページ）を参照してください。

関連項目

- メッセージがスパムかどうかスキャンするためのアプライアンス の設定方法 （2 ページ）

リレーされたメッセージのメッセージ ヘッダー

リレーされたメッセージの元の送信者の識別にヘッダーのタイプが次のいずれかを使用するようにアプライアンス を設定します。

- カスタム ヘッダー （42 ページ）
- Received ヘッダー （42 ページ）

カスタム ヘッダー

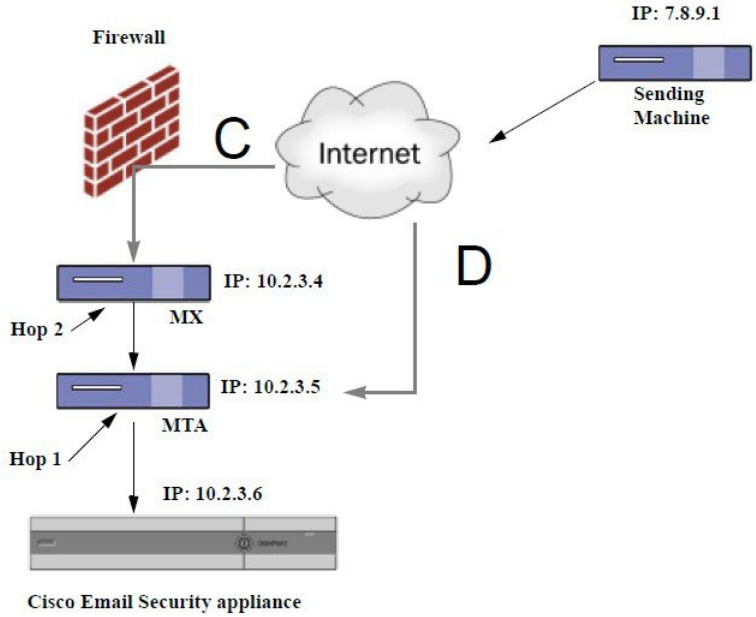
カスタムヘッダーを使用して元の送信者を識別する推奨される方法です。元の送信者に接続するマシンでは、このカスタムヘッダーを追加する必要があります。このヘッダーの値は、外部の送信マシンの IP アドレスになることが予期されます。例：

```
SenderIP: 7.8.9.1
```

```
X-CustomHeader: 7.8.9.1
```

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、次の図では、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 : MX/MTA* によるメール リレー：不定ホップ数



関連項目

- 着信リレーの追加　（40 ページ）

Received ヘッダー

MX/MTA を設定する際に、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らない場合、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」の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：*MX/MTA* によるメール リレー：拡張」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。受信メールがお使いのアプライアンスに接続しているマシンへの別のパスを取ることができる場合（「図：*MX/MTA*

によるメールリレー：不定ホップ数」で説明しているように、異なるホップ数になる）、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 （42 ページ）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（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、使用するヘッダーを指定するログの設定 （47 ページ）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、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す。解析対象文字も有効な IP アドレスも見つからない場合、アプライアンス は接続マシンの実際の IP アドレスを使用します。

次の例のメール ヘッダーの場合、左角カッコ（[）と 2 ホップを指定した場合は、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：*MX/MTA* によるメール リレー：拡張」の例で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）

「図：*MX/MTA* によるメールリレー：拡張」に示すように、アプライアンスまでにいくつかのホップを通過するメッセージの電子メールヘッダーの例を次の表に示します。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（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 *1*：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 ESMTP; 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 ESMTP id j8LKkWu1008155 for`
	`<joefoo@customerdomain.org>`

4	`Received: from sending-machine.spamham.com (sending-machine.spamham.com [7.8.9.1])`
	`by mx.customerdomain.org (Postfix) with ESMTP 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 ESMTP; Received: from exchange1.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>

上記の表のメモ：

- アプライアンス では、これらのヘッダーを無視します。
- 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）。
- 最初のホップ（着信リレー）。
- 第 2 ホップ。これは、送信側 MTA です。IP アドレスは 7.8.9.1 です。
- 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。

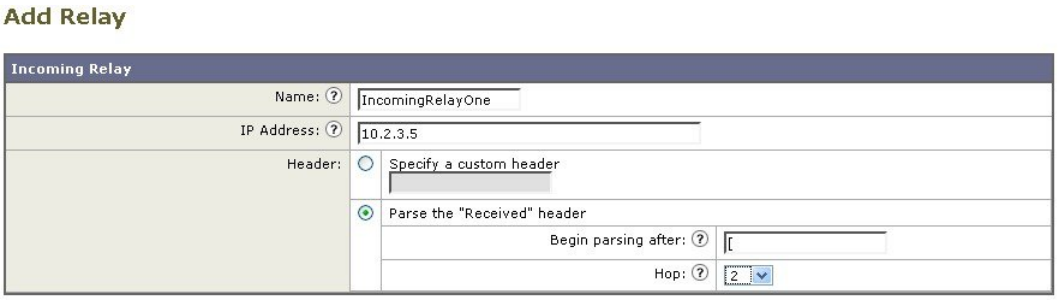
次の表に、外部ヘッダーを除く、同じ電子メール メッセージのヘッダーを示します

表 *2：*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 ESMTP; 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 ESMTP 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 ESMTP id 4F3DA15AC22 for <joefoo@customerdomain.org>;

次の図 に、GUI の [リレーの追加（Add Relay）] ページで設定されたパス A（前述）の着信リレーを示します。

図 *9 : Received* ヘッダー付きで設定された着信リレー



関連項目

- 着信リレーの追加 （40 ページ）

着信リレーが機能にどのように影響するか

着信リレーとフィルタ

着信リレー機能では、IP レピュテーションサービスに関連するさまざまなフィルタルール（reputation、no-reputation）にさまざまな IP レピュテーションスコアを提供します。

着信リレー、HAT、IP レピュテーションスコア、および送信者グループ

HAT ポリシー グループは、着信リレーからの情報は現在は使用していません。ただし、着信リレー機能では レピュテーションスコアが提供されるため、メッセージフィルタおよび $reputation 変数を使用して HAT ポリシーグループ機能をシミュレートできます。

着信リレーおよびディレクトリ ハーベスト攻撃防止

リモートホストが、ネットワーク上で着信リレーとして使われている MX または MTA にメッセージを送ることでディレクトリ獲得攻撃防止を試みる場合、アプライアンスは、ディレクトリ獲得攻撃防止（DHAP）がイネーブルに設定されたメールフローポリシーを持つ送信者グループにリレーが割り当てられていると、その着信リレーからの接続をドロップします。これは、リレーからすべてのメッセージが、正規のメッセージも含めアプライアンスに接続されないよう防止します。アプライアンスはリモートホストが攻撃者であると認識できず、着信リレーとして機能する MX または MTA は攻撃元ホストからメールを受信し続けます。この問題を回避

して、着信リレーからメッセージを受信し続けるために DHAP の無制限のメッセージがあるメール フロー ポリシーを送信者グループにリレーを追加します。

着信リレーおよびトレース

トレースは、送信元 IP アドレスのレピュテーションスコアの代わりに、結果の着信リレーの IP レピュテーションスコアを返します。

着信リレーと電子メール セキュリティ モニタ（レポート）

着信リレーを使用する場合：

- 電子メール セキュリティ モニタ レポートには外部 IP および MX/MTA の両方のデータが含まれます。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、[メールフローサマリー（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。
- IP レピュテーションスコアは、電子メール セキュリティ モニタ レポートで正しく報告されません。送信者グループが正しく解決されない場合もあります。

着信リレーおよびメッセージ トラッキング

着信リレーを使用すると、メッセージトラッキングの詳細ページに、外部送信元の IP アドレスおよびレピュテーションスコアの代わりに、メッセージのリレーの IP アドレスおよびリレーの IP レピュテーションスコアが表示されます。

着信リレーとロギング

次のログの例で、送信者の IP レピュテーショスコアは、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 IP レピュテーションスコアが 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 IPR 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, IPR **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

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
```

使用するヘッダーを指定するログの設定

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のみ検査します。したがって、ローカルで追加されるヘッダー（Microsoft Exchange のヘッダーなど）や、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、使用するヘッダーを AsyncOS ロギングに含めるよう設定することです。

ヘッダーのロギング設定を設定するには、ロギングのグローバル設定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

使用許諾契約に同意すると、最新の Cisco Anti-Spam および Cisco Intelligent Multi-Scan ルールのアップデートを確認できます。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [IronPort Anti-Spam] を選択します。

または

ステップ 2 [セキュリティサービス（Security Services）] > [IMSおよびグレイメール（IMS and Graymail）] を選択します。

ステップ 3 [ルールの更新（Rule Updates）] セクションを表示し、次を行います。

目的 (To)	詳細情報
各コンポーネントの最新の更新について参照	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。
アップデートが使用可能かどうかを確認	—
アップグレードが入手可能な場合はルールを更新	[今すぐ更新（Update Now）] をクリックします。

次のタスク

関連項目

- サービス アップデート
- プロキシ サーバを経由したアップデート
- アップグレードおよびアップデートをダウンロードするためのサーバ設定

スパム対策のテスト

目的	操作手順	詳細情報
設定をテストします。	`X-advertisement: spam` ヘッダーを使用して、設定をテストします。 テストを目的として、Cisco 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、Cisco 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（スパム対策ポリシーの定義 （22 ページ））が実行されることを確認できます。 次のいずれかをこのヘッダーに使用します。 • このヘッダーを含むテストメッセージを送信する SMTP コマンドを使用します。Cisco Anti-Spam をテストするためのアプライアンス へのメール送信 （49 ページ）を参照してください。 • trace コマンドを使用してこのヘッダーを含めます。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。

目的	操作手順	詳細情報
スパム対策エンジンの有効性を評価します。	インターネットから直接本物のメール ストリームを使用して製品を評価します。	回避すべき非効率的な評価のアプローチの一覧については、スパム対策の有効性をテストできない方法 （50 ページ）を参照してください。

関連項目

- Cisco Anti-Spam をテストするためのアプライアンス へのメール送信 （49 ページ）
- スパム対策の有効性をテストできない方法 （50 ページ）

Cisco Anti-Spam をテストするためのアプライアンス へのメール送信

はじめる前に

スパム対策設定のテスト：SMTP の使用例 （50 ページ）の例を確認してください。

手順

ステップ 1 メール ポリシーで Cisco Anti-Spam を有効にします。

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。

Telnet で SMTP コマンドを使用して、アクセスできるアドレスにこのメッセージを送信します。

ステップ 3 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。

次に例を示します。

- 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。

関連項目

- スパム対策設定のテスト：SMTP の使用例 （50 ページ）

スパム対策設定のテスト：SMTP の使用例

この例では、テスト アドレスのメッセージを受信するようにメール ポリシーを設定し、HAT でテスト接続を許可する必要があります。

```
# telnet IP_address_of_IronPort_Appliance_with_IronPort_Anti-Spam port

220 hostname ESMTP

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
```

スパム対策の有効性をテストできない方法

IronPort Anti-Spam と Cisco 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、次の方法のいずれかを使用して有効性をテストしないでください。

- 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」だけをテストする。

  IP レピュテーションサービス、ブロックリスト、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。

- 別のスパム対策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。

  スキャンエンジンは現在の脅威に基づき、迅速にルールを追加し、排除します。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。