スパム対策

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 （1 ページ）
- 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）
- IronPort スパム対策フィルタリング （4 ページ）
- Cisco Intelligent Multi-Scan のフィルタリング （7 ページ）
- スパム対策ポリシーの定義 （8 ページ）
- 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 （16 ページ）
- スパム対策スキャン中に追加されるヘッダー （16 ページ）
- 誤って分類されたメッセージのシスコへの報告 （16 ページ）
- 着信リレー構成における送信者の IP アドレスの決定 （21 ページ）
- モニタリング ルールのアップデート （30 ページ）
- スパム対策のテスト （31 ページ）

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。
    - スパムでない
    - 陽性と疑わしいスパム
    - 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。

スパム対策ソリューション

Cisco 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）.
- Cisco Intelligent Multi-Scan のフィルタリング （7 ページ）.

Cisco 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	E メール セキュリティ 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。 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） • Cisco Intelligent Multi-Scan のフィルタリング （7 ページ）

	コマンドまたはアクション	目的
ステップ 2	ローカルの E メール セキュリティ アプライアンスからスパムを隔離するか、または、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 （8 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）SenderBase 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、SenderBase レピュテーション スコアを各受信メール フロー ポリシーにイネーブルにします。	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	E メール セキュリティ 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 （21 ページ）
ステップ 8	アプライアンスで正しく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 （16 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 （31 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

評価キー

Cisco 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。

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。

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。

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 によるメッセージの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。
リージョナル スキャン（Regional Scanning）	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。該当する場合は、地域を選択します。 指定した地域から大量の電子メールを受信した場合にのみこの機能をイネーブルにします。この機能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。

Cisco Intelligent Multi-Scan のフィルタリング

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） 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。

Cisco Intelligent Multi-Scan の設定

（注） 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。

はじめる前に

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。

ステップ 1 [セキュリティサービス（Security Services）]>[IronPortインテリジェントマルチスキャン（IronPort Intelligent Multi-Scan）] 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 [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 [インテリジェントマルチスキャンを有効にする（Enable Intelligent Multi-Scan）] 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。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。

ステップ 5 Cisco Intelligent Multi-Scan 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。
- 1 M 超はスキャンしないでください。

ステップ 6 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 スループットを最適化できる可能性があります。

ステップ 7 変更を送信し、保存します。

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 （11 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 （12 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 （12 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 （14 ページ）
  - スパム対策スキャン中に追加されるヘッダー （16 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。

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。

オプション	説明
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） • 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。
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 （13 ページ）を参照してください。

オプション	説明
（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。

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。

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。グレイメールの管理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。

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。

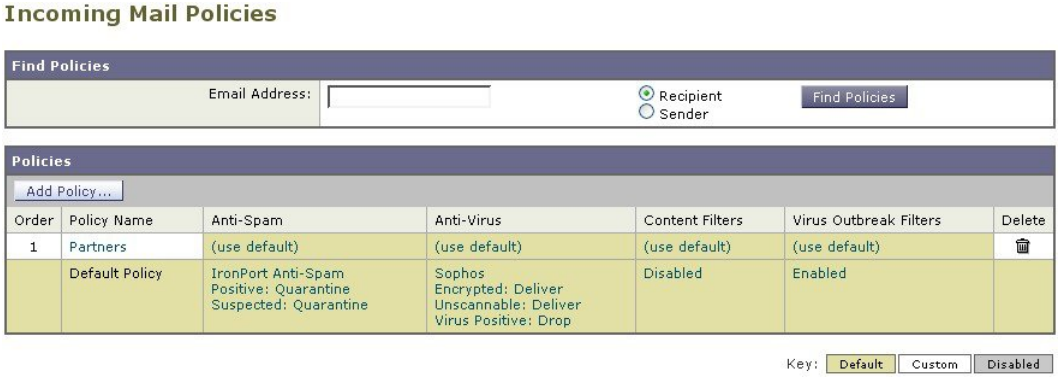
異なるメール ポリシーでの異なるスパム対策スキャン エンジンの有効化：設定例

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 *1:* メール ポリシー：受信者ごとのスパム対策エンジン

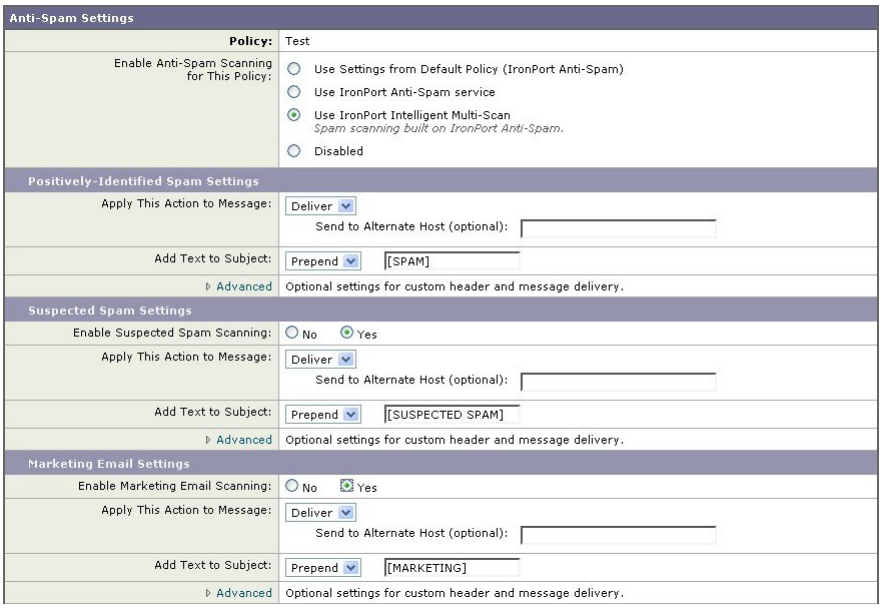


パートナーのポリシーを変更して、不要なマーケティング メッセージに対して Cisco Intelligent Multi-Scan とスキャンを使用するには、パートナーの行に対応する [スパム対策（Anti-Spam）] 列のエントリ（[デフォルトを使用（Use Default）]）をクリックします。

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 *2 :* 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 *3 :* 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

Cisco IronPort 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 （8 ページ）を参照してください。

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

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。

ステップ 1 組織内すべてのアプライアンスに共通の登録 ID を設定します。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。

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）] > [電子メール送信およびトラッキング ポータル登録（Email Submission and Tracking 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）] フィールドに値を入力します。入力する値は、16 文字以上 48 文字以下として、英数字、ハイフン（-）、およびアンダースコア（_）のみで構成する必要があります。
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。

ステップ 2 シスコ電子メール送信およびトラッキング ポータルでの管理者としての登録は、次のいずれかの方法で実行できます。シスコ電子メール送信およびトラッキング ポータルは、電子メール管理者が間違って分類されたメッセージをシスコに報告して追跡できる Web ベースのツールです。

（注） シスコ電子メール送信およびトラッキング ポータルは Web ベースのツールであり、電子メール管理者は誤って分類されたメッセージをシスコに報告してそれらを追跡できます。

- 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. Cisco クレデンシャルを使用して、Cisco SecurityHub（https://securityhub.cisco.com/）にログインします。
  2. [電子メールの送信およびトラッキング（）] をクリックします。
  3. 電子メール送信およびトラッキング ポータルで、[新しい登録IDを登録する（Register a new Registration ID）] を選択し、**ステップ 1** で作成した登録 ID を入力して、[登録（Register）] をクリックします。ここで入力する登録 ID は、アプライアンスでの電子メール送信およびトラッキング ポータルの設定中に入力したのと必ず同じものにします。

- 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. Cisco クレデンシャルを使用して、Cisco SecurityHub（https://securityhub.cisco.com/）にログインします。

2. [電子メールの送信およびトラッキング（）] をクリックします。
3. 電子メール送信およびトラッキング ポータルで、[管理者として登録（Register as an administrator）] を選択し、ポータルに登録済みの管理者の電子メール アドレスを入力して、[登録（Register）] 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。管理者はポータルにログインし、設定パネルで [管理者登録要求（Admin registration requests）] をクリックして、登録要求を許可または拒否する必要があります。

ステップ 3 シスコ電子メール送信およびトラッキング ポータルに登録します。

1. シスコ電子メール送信およびトラッキング ポータルに移動します。
2. [構成（Configuration）] > [ドメイン（Domains）] をクリックします。
3. [新規ドメインを追加（Add new domain）] をクリックします。
4. 組織のドメインを入力して、[追加（Add）] をクリックします。

（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。

ドメインの追加要求は `postmaster@domain.com` に送信されます。ここで domain.com はこのステップで入力したドメインを示しています。このドメインからの管理者は、要求を確認して承認します。

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"); }
```

誤って分類されたメッセージのシスコへの報告方法

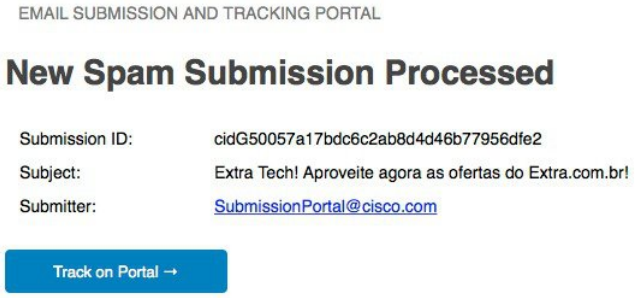
詳細については、https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200648-ESA-FAQ-How-to-work-with-Cisco-Email-Su.html を参照してください。

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 （17 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 （19 ページ）
- シスコ電子メール送信およびトラッキング ポータルの使用 （19 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 （20 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、2 時間以内に電子メール通知が届きます。次に示すのは、電子メール通知の例です。



電子メール通知が 2 時間以内に届かない場合は、送信が失敗している可能性があります。トラブルシューティングの手順については、ポータルで、[ヘルプ（Help）] > [トラブルシューティングの手順（Troubleshooting Instructions）] をクリックしてください。

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。

シスコ電子メール送信およびトラッキング ポータルの使用

シスコ電子メール送信およびトラッキング ポータルは、メール管理者が、誤って分類されたメッセージをシスコへ報告することができる Web ベースのツールです。管理者は、ポータルを使用して、組織からの送信も追跡できます。

（注） 現在、ポータルを使用して、誤って分類されたスパム メッセージのみ報告できます。

ステップ 1 Cisco クレデンシャルを使用して、Cisco SecurityHub（https://securityhub.cisco.com/）にログインします。

ステップ 2 [電子メールの送信およびトラッキング（）] をクリックします。

ステップ 3 電子メール送信およびトラッキング ポータルの [送信（Submissions）] タブで、[新しい送信（New Submission）] をクリックします。

ステップ 4 誤って分類されたメッセージを選択します。これらのメッセージはEML形式である必要があり、メッセージの合計サイズが 15 MB を超えてはいけません。

ステップ 5 [作成（Create）] をクリックします。

次のタスク

その他の情報

シスコ電子メール送信およびトラッキングポータルの詳細については、次のドキュメントを参照してください。

方法	参照先：
電子メール送信およびトラッキング ポータルを使用して、誤って分類されたメッセージをシスコに報告	https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117822-qanda-esa-00.html
シスコ電子メール送信およびトラッキング ポータルの操作	https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200648-ESA-FAQ-How-to-work-with-Cisco-Email-Su.html
シスコ電子メール送信およびトラッキング ポータルのトラブルシューティング	https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200653-ESA-FAQ-Troubleshooting-Email-Submissio.html

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。

- 見逃されたスパム：spam@access.ironport.com
- メッセージはスパムとしてマークされたがスパムではない ham@access.ironport.com
- 見逃されたマーケティング メッセージ ads@access.ironport.com
- メッセージはマーケティング 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 not_ads@access.ironport.com
- 見逃されたフィッシング メッセージ phish@access.ironport.com

メッセージを転送するのに次の電子メールプログラムのいずれかを使用すると、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、シスコ電子メール送信およびトラッキング ポータルで送信を表示および追跡できます。

ステップ 1 Cisco のクレデンシャルを使用して、Cisco SecurityHub にログインします（https://securityhub.cisco.com/)）。
ステップ 2 [電子メールの送信およびトラッキング（）] をクリックします。
ステップ 3 電子メール送信およびトラッキング ポータルで、[送信（Submissions）] をクリックします。
ステップ 4 フィルタ（期間、送信 ID、件名、送信者、およびステータス）を使用して送信を検索します。

次のタスク

詳細については、https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200648-ESA-FAQ-How-to-work-with-Cisco-Email-Su.html.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

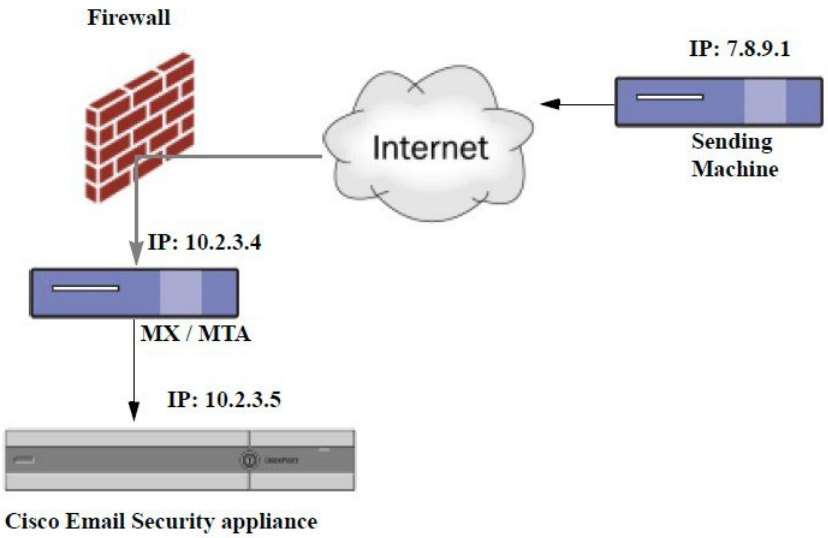
1 つ以上のメール交換/転送エージェント（MX または MTA）、フィルタ サービスが Cisco アプライアンスと着信メールを送信する外部マシンとの間のネットワークのエッジに配置されている場合、アプライアンスは送信元マシンの IP アドレスを決定することはできません。代わりに、メールはローカル MX/MTA から送信されたように見えます。ただし、IronPort Anti-Spam および Cisco Intelligent Multi-Scan（SenderBase レピュテーション サービスを使用）は外部送信者の正確な IP アドレスに依存します。

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。Cisco 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。

着信リレーを使用した環境例

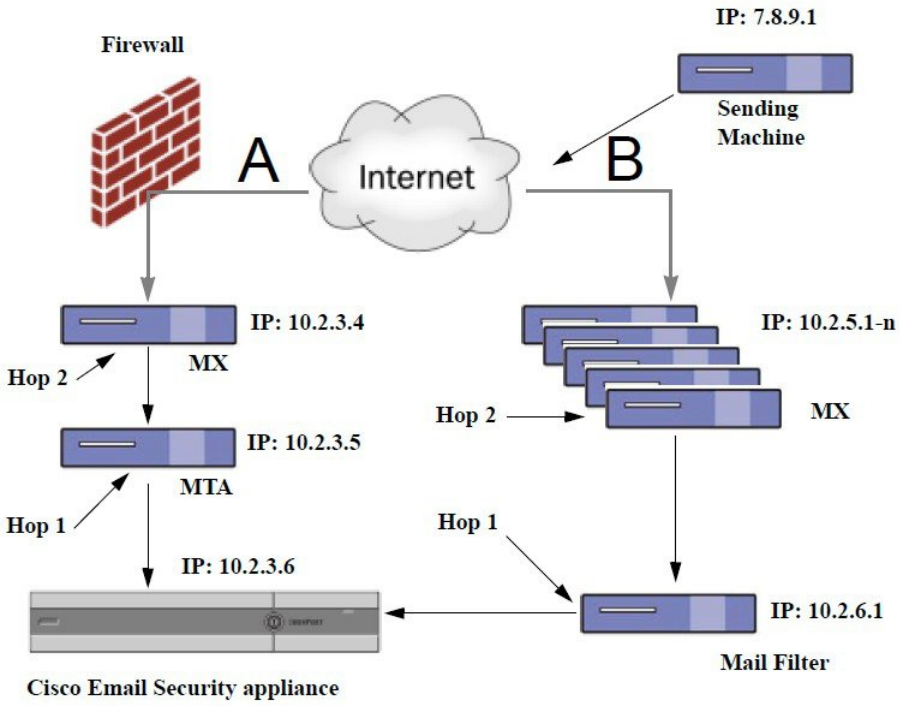
次の図に、着信リレーの非常に基本的な例を示します。ローカル MX/MTA によってメールが Cisco アプライアンスにリレーされているため、IP アドレス 7.8.9.1 からのメールは IP アドレス 10.2.3.4 からのように見えます。

図 *4 : 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、Cisco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、Cisco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、Ciscoアプライアンスに配信されます。

図 *5 : 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

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 Cisco アプライアンスにリレーする場合のみ、着信リレー機能を有効にしてください。

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。

- E メール セキュリティ 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（25 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。

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 E メール セキュリティ 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 （29 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 （30 ページ）を参照してください。

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

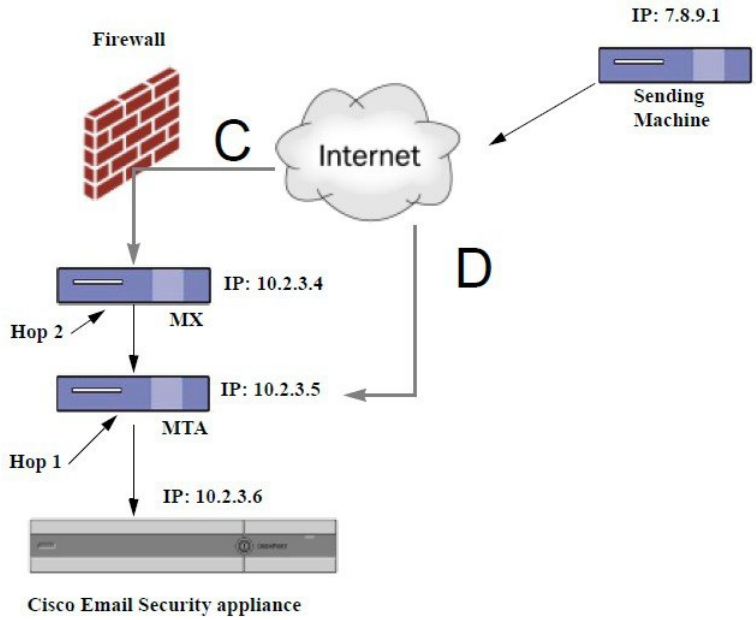
カスタムヘッダーを使用して元の送信者を識別する推奨される方法です。元の送信者に接続するマシンでは、このカスタムヘッダーを追加する必要があります。このヘッダーの値は、外部の送信マシンの IP アドレスになることが予期されます。次に例を示します。

```
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 *6 : 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 Cisco 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 （25 ページ）を参照してください）。

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（Cisco 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 （30 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、Cisco 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、Cisco 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、Cisco 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（Cisco 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：

- Cisco アプライアンスでは、これらのヘッダーを無視します。
- Cisco 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。
- Cisco 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。

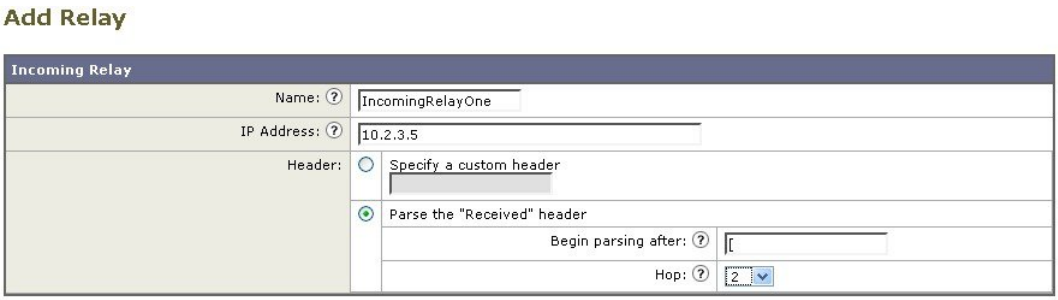
次の表に、外部ヘッダーを除く、同じ電子メール メッセージのヘッダーを示します

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 *7: Received* ヘッダー付きで設定された着信リレー



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、SenderBase 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）に正しい SenderBase レピュテーション 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 SenderBase レピュテーション 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 E メール セキュリティ 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 SenderBase 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。
- SenderBase 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、元の外部送信者の 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側 SenderBase 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 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 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 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

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

Cisco 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、Cisco 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。

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）]>[IronPortインテリジェントマルチスキャン（IronPort Intelligent Multi-Scan）] 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	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。

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 （8 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 （32 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。
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 （33 ページ）を参照してください。

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 （32 ページ）の例を確認してください。

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。

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。

  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。