



スパム隔離

この章は、次の項で構成されています。

- [スパム隔離の概要 \(1 ページ\)](#)
- [ローカルのスパム隔離と外部のスパム隔離 \(2 ページ\)](#)
- [中央集中型スパム隔離の設定 \(2 ページ\)](#)
- [\[スパム隔離の編集 \(Edit Spam Quarantine\)\] ページ \(9 ページ\)](#)
- [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 \(9 ページ\)](#)
- [エンドユーザーのためのスパム管理機能の設定 \(23 ページ\)](#)
- [スパム隔離内のメッセージの管理 \(34 ページ\)](#)
- [スパム隔離のディスク領域 \(37 ページ\)](#)
- [外部スパム隔離の無効化について \(37 ページ\)](#)
- [スパム隔離機能のトラブルシューティング \(37 ページ\)](#)

スパム隔離の概要

スパム隔離 (別名 ISQ) およびエンドユーザー隔離 (別名 EUQ) は、「誤検出」 (アプライアンスが正規の電子メールメッセージをスパムと見なすこと) が問題とされる組織でのセーフガードメカニズムとなります。メッセージがスパムである、またはスパムの疑いがあるとアプライアンスが判断した場合、メッセージを配信または削除する前に、受信者または管理者にそのメッセージを確認してもらうことができます。スパム隔離はこのためにメッセージを保存します。

Eメールセキュリティアプライアンスの管理ユーザは、スパム隔離内のすべてのメッセージを閲覧できます。エンドユーザ (通常はメッセージの受信者) は、そのユーザ宛の隔離されたメッセージを、若干異なる Web インターフェイスで表示できます。

スパム隔離は、ポリシー、ウイルス、アウトブレイク隔離とは異なります。

関連項目

- [集約されたポリシー、ウイルス、およびアウトブレイク隔離](#)

ローカルのスパム隔離と外部のスパム隔離

ローカルのスパム隔離では、Eメールセキュリティ アプライアンスでスパムおよびスパムの疑いがあるメッセージなどを保存します。外部のスパム隔離は、別のCisco コンテンツセキュリティ管理アプライアンスでこれらのメッセージを保存できます。

次の場合は外部のスパム隔離の使用を検討してください。

- 複数のEメールセキュリティ アプライアンスからのスパムを集約して保存および管理する必要がある。
- Eメールセキュリティ アプライアンスで保持可能な量より多くのスパムを保存する必要がある。
- スパム隔離とそのメッセージを定期的にバックアップする必要がある。

中央集中型スパム隔離の設定


手順

	コマンドまたはアクション	目的
ステップ 1	セキュリティ管理アプライアンスで、中央集中型スパム隔離を有効にします。	スパム隔離の有効化と設定 (3 ページ)
ステップ 2	セキュリティ管理アプライアンスで、中央集中型スパム隔離に含めるEメールセキュリティ アプライアンスを指定します。	管理対象の各Eメールセキュリティ アプライアンスへの中央集中型スパム隔離サービスの追加 (5 ページ)
ステップ 3	通知およびリリースされたスパムの送信用にセキュリティ管理アプライアンスを設定します。	セキュリティ管理アプライアンスでの発信 IP インターフェイスの設定 (6 ページ)
ステップ 4	セキュリティ管理アプライアンスで、スパム隔離ブラウザ インターフェイスを設定します。	スパム隔離へのブラウザアクセス用 IP インターフェイスの設定 (7 ページ)
ステップ 5	Eメールセキュリティアプライアンスがスパム隔離にメールを送信するように設定されていることを確認します。	スパム対策およびメールポリシーの設定の詳細については、『 User Guide for AysncOS for Email Security Appliances 』の「Anti-Spam」セクションを参照してください。
ステップ 6	Eメールセキュリティアプライアンスで外部スパム隔離を有効にし、設定します。	詳細については、『 User Guide for AysncOS for Email Security Appliances 』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で、内部隔離を無効にします。	外部スパム隔離をアクティブ化するためのローカルスパム隔離の無効化に関する詳細については、『 User Guide for AysncOS for Email Security Appliances 』を参照してください。

スパム隔離の有効化と設定

- レガシー Web インターフェイスでのスパム隔離の有効化と設定 (3 ページ)

レガシー Web インターフェイスでのスパム隔離の有効化と設定

- ステップ 1** (新しい Web インターフェイスのみ) セキュリティ管理アプライアンスで  をクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [集約サービス (Centralized Services)] > [スパム隔離 (Spam Quarantine)] を選択します。
- ステップ 3** システムセットアップウィザードの実行後、スパム隔離を初めて有効にする場合は、次の手順を実行します。
- [有効 (Enable)] をクリックします。
 - エンド ユーザ ライセンス契約書を確認し、[承認 (Accept)] をクリックします。
- ステップ 4** スпам隔離の設定を編集する場合は、[設定の編集 (Edit Settings)] をクリックします。
- ステップ 5** 次のオプションを指定します。

オプション	説明
隔離IPインターフェイス (Quarantine IP Interface) 隔離ポート (Quarantine Port)	デフォルトでは、スパム隔離は管理インターフェイスとポート 6025 を使用します。IP インターフェイスは、着信メールをリッスンするように設定されているセキュリティ管理アプライアンスのインターフェイスです。隔離ポートは、送信アプライアンスが外部隔離設定で使用しているポート番号です。 E メール セキュリティ アプライアンスがセキュリティ管理アプライアンスと同じネットワークに存在しない場合、管理インターフェイスを使用する必要があります。

オプション	説明
<p>[次を使用してメッセージを配信 (Deliver Messages Via)]</p>	<p>隔離関係のすべての送信電子メール（スパム通知やスパム隔離からリリースされたメッセージなど）は、メッセージ送信が設定されている他のアプライアンスまたはサーバを経由して配信する必要があります。</p> <p>これらのメッセージは、SMTPまたはグループウェアサーバを使用してルーティングできます。また、Eメールセキュリティアプライアンスの発信リスナー インターフェイス（通常は Data 2 インターフェイス）を指定することもできます。</p> <p>代替用アドレスは、ロードバランシングとフェールオーバーに使用します。</p> <p>Eメールセキュリティアプライアンスが複数台ある場合は、管理対象の任意のEメールセキュリティアプライアンスの発信リスナー インターフェイスをプライマリ アドレスまたは代替用アドレスとして使用できます。これらはいずれも同じインターフェイス（Data 1 または Data 2）を発信リスナーとして使用する必要があります。</p> <p>これらのアドレスについての他の注意事項を画面で確認してください。</p>
<p>次の日数の経過後に削除 (Schedule Delete After)</p>	<p>メッセージを削除する前に保持する日数を指定します。</p> <p>隔離エリアの容量が満杯になるのを防ぐために、古いメッセージから削除するように隔離を設定することを推奨します。自動削除をスケジュールしないという選択も可能です。</p>
<p>[メッセージのリリース時にCiscoに通知 (Notify Cisco Upon Message Release)]</p>	<p>メッセージのリリース時にシスコに通知する場合は、[Send a copy of released messages To cisco for analysis (推奨)] チェックボックスをオンにします。</p>

オプション	説明
[スパム隔離のアピアランス (Spam Quarantine Appearance)]	<p>ロゴ (Logo)</p> <p>デフォルトでは、ユーザがログインして隔離されたメッセージを確認するときに、スパム隔離のページの最上部にシスコロゴが表示されます。</p> <p>ロゴは、新しい Web インターフェイスとレガシー Web インターフェイスの両方で表示できます。</p> <p>代わりにカスタムロゴを使用するには、そのロゴをアップロードします。ロゴは、高さ 50 ピクセル、幅 500 ピクセルまでの .jpg、.gif、または .png ファイルにする必要があります。</p> <p>ログインページメッセージ (Login page message)</p> <p>(任意) ログインページメッセージを指定します。このメッセージは、隔離を閲覧するためにエンドユーザおよび管理者がログインするときに表示されます。</p> <p>メッセージを指定しない場合、次のメッセージが表示されます。</p> <p>ログイン情報を入力してください。入力する情報がわからない場合は、管理者に問い合わせてください。(Enter your login information below. If you are unsure what to enter, please contact your administrator.)</p>
管理ユーザ (Administrative Users)	<p>スパム隔離への管理ユーザアクセスの設定 (8 ページ) を参照してください。</p>


ステップ 6 変更を送信し、保存します。

次のタスク

- [管理対象の各 E メールセキュリティ アプライアンスへの中央集中型スパム隔離サービスの追加 \(5 ページ\)](#) に戻ります。

管理対象の各 E メールセキュリティ アプライアンスへの中央集中型スパム隔離サービスの追加

ここで実行する手順は、他の中央集中型管理機能の設定時に、すでにこのアプライアンスを追加したかどうかによって異なります。

ステップ 1 (新しい Web インターフェイスのみ) セキュリティ管理アプライアンスで  をクリックして、レガシー Web インターフェイスをロードします。

- ステップ 2** [管理アプライアンス (Management Appliance)]>[集約管理サービス (Centralized Services)]>[セキュリティアプライアンス (Security Appliances)]を選択します。
- ステップ 3** このページのリストに、すでに E メールセキュリティアプライアンスを追加している場合は、次の手順を実行します。
- E メールセキュリティアプライアンスの名前をクリックします。
 - [スパム隔離 (Spam Quarantine)] サービスを選択します。
- ステップ 4** E メールセキュリティアプライアンスをまだ追加していない場合は、次の手順を実行します。
- [メールアプライアンスの追加 (Add Email Appliance)] をクリックします。
 - [アプライアンス名 (Appliance Name)] および [IP アドレス (IP Address)] テキストフィールドに、アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。
- (注) [IP アドレス (IP Address)] フィールドに DNS 名を入力した場合でも、[送信 (Submit)] をクリックすると、IP アドレスに変換されます。
- Spam Quarantine サービスが事前に選択されています。
 - [接続の確立 (Establish Connection)] をクリックします。
 - 管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立 (Establish Connection)] をクリックします。
- (注) ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモートアプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は Security Management Appliance に保存されません。
- 「Success」メッセージがページのテーブルの上に表示されるまで待機します。
 - [テスト接続 (Test Connection)] をクリックします。
 - テーブルの上のテスト結果を確認します。
- ステップ 5** 変更を送信し、保存します。
- ステップ 6** スпам隔離を有効にする E メールセキュリティアプライアンスごとに、この手順を繰り返します。

セキュリティ管理アプライアンスでの発信 IP インターフェイスの設定


セキュリティ管理アプライアンスで、隔離に関するメッセージ（通知やリリースされた電子メールなど）を E メールセキュリティアプライアンスに送信するインターフェイスを設定します。

始める前に

発信インターフェイスに使用する IP アドレスを入手または特定します。通常、これはセキュリティ管理アプライアンスの Data2 インターフェイスのものになります。ネットワーク要件の詳細については、を参照してください。 [ネットワークと IP アドレスの割り当て](#)



(注) この手順は、[IP インターフェイスの設定](#)の説明と併せて実行してください。

- ステップ 1** (新しい Web インターフェイスのみ) セキュリティ管理アプライアンスで  をクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)]>[ネットワーク IP インターフェイス (Network IP Interfaces)] を選択します。
- ステップ 3** [IP インターフェイスの追加 (Add IP Interface)] をクリックします。
- ステップ 4** 次の設定値を入力します。

- [名前 (Name)]
- イーサネット ポート (Ethernet Port)

通常は Data 2 になります。具体的には、この設定は [管理アプライアンス (Management Appliance)]> [集約管理サービス (Centralized Services)]> [スパム隔離 (Spam Quarantine)] の [スパム隔離設定 (Spam Quarantine Settings)] ページにおいて、[次を使用してメッセージを配信 (Deliver Messages Via)] セクションで [プライマリサーバ (Primary Server)] に指定した E メールセキュリティ アプライアンスのデータ インターフェイスと同じである必要があります。


- [IP アドレス (IP Address)]
上で指定したインターフェイスの IP アドレス。
- ネットマスク
- ホストネーム
たとえば、Data 2 インターフェイスの場合は、data2.sma.example.com を使用します。

このインターフェイスの [スパム隔離 (Spam Quarantine)] セクションには入力しないでください。

- ステップ 5** 変更を送信し、保存します。

スパム隔離へのブラウザ アクセス用 IP インターフェイスの設定

管理者およびエンド ユーザがスパム隔離にアクセスするときには、別のブラウザ ウィンドウが開きます。

- ステップ 1** (新しい Web インターフェイスのみ) セキュリティ管理アプライアンスで  をクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)]>[ネットワーク (Network)]> [IP インターフェイス (IP Interfaces)] を選択します。
- ステップ 3** 管理インターフェイスの名前をクリックします。
- ステップ 4** [スパム隔離 (Spam Quarantine)] セクションで、スパム隔離にアクセスするための設定を行います。
- デフォルトでは、HTTP がポート 82 を使用し、HTTPS がポート 83 を使用します。

- 通知とスパム隔離のブラウザ ウィンドウに記載される URL を指定します。

使用しているセキュリティ管理アプライアンスのホスト名をエンドユーザに表示したくない場合は、代わりのホスト名を指定できます。

ステップ 5 変更を送信し、保存します。

次のタスク

スパム隔離アクセス用に指定したホスト名を DNS サーバが解決できることを確認します。

スパム隔離への管理ユーザアクセスの設定

管理者権限を持つすべてのユーザは、スパム隔離設定を変更したり、スパム隔離内のメッセージを表示および管理したりすることができます。管理者ユーザに対してスパム隔離アクセスを設定する必要はありません。


次のロールのユーザに対してスパム隔離へのアクセスを設定すると、これらのユーザはスパム隔離内のメッセージを表示、リリース、削除できます。

- Email administrator
- 演算子
- Read-Only Operator
- Help desk user
- ゲスト
- スパム隔離権限を持つカスタム ユーザ ロール

これらのユーザはスパム隔離設定にアクセスできません。

始める前に

スパム隔離にアクセスできるユーザまたはカスタム ユーザ ロールを作成します。詳細については、の項で[カスタム ユーザ ロールの隔離へのアクセス](#)に関する情報[管理タスクの分散](#)を参照してください。

ステップ 1 セキュリティ管理アプライアンスで、[サービスステータス (Service Status)] をクリックし、[スパム隔離 (Spam Quarantine)] に対応する  にカーソルを合わせて、[スパム隔離設定の編集 (Edit Spam Quarantine Settings)] をクリックします。

ステップ 2 トグルスイッチをクリックしてスパム隔離を有効にします。

ステップ 3 追加するユーザタイプ (ローカル、外部認証、またはカスタム ロール) のリンクをクリックします。

ユーザまたはロールを追加済みの場合は、ユーザ名かロールをクリックすると、すべての対象ユーザまたはロールが表示されます。

ステップ 4 追加するユーザまたはロールを選択します。

管理者権限を持つユーザ（電子メール管理者を含む）は、スパム隔離へのフルアクセスが自動的に与えられるため、表示されません。

ステップ5 [OK] をクリックします。

ステップ6 [送信 (Submit)] をクリックします。

次のタスク

関連項目

[スパム隔離へのエンドユーザ アクセスの設定 \(26 ページ\)](#)

隔離対象のメールの受信者の制限

複数のメール ポリシーを使用して ([メールポリシー (Mail Policies)] > [受信メールポリシー (Incoming Mail Policy)])、メールの隔離対象から除外する受信者アドレスのリストを指定できます。そのメールポリシーにアンチスパムを設定する際、隔離の代わりに [配信 (Deliver)] または [ドロップ (Drop)] を選択します。

スパム隔離の言語

各ユーザは、ウィンドウの右上にある [オプション (Options)] メニューからスパム隔離の言語を選択します。

[スパム隔離の編集 (Edit Spam Quarantine)] ページ

- [レガシー Web インターフェイスでのスパム隔離の有効化と設定 \(3 ページ\)](#)
- [ローカルのスパム隔離と外部のスパム隔離 \(2 ページ\)](#)
- [スパム隔離へのエンドユーザ アクセスの設定 \(26 ページ\)](#)
- [エンドユーザへの隔離されたメッセージに関する通知 \(29 ページ\)](#)

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

管理者およびエンドユーザは、メッセージがスパムであるかどうかを判断するためにセーフリストとブロックリストを使用できます。セーフリストでは、スパムとして処理しない送信者およびドメインが指定されます。ブロックリストでは、常にスパムとして処理する送信者およびドメインが指定されます。

エンドユーザ（電子メールユーザ）に各自の電子メールアカウントのセーフリストとブロックリストの管理を許可することができます。たとえば、エンドユーザは、もう興味のないメーリングリストから電子メールを受信している場合があります。そのようなユーザは、このメー

リングリストからの電子メールが自分の受信箱に送信されないように、その送信者を自分のブロックリストに追加できます。また、エンドユーザは、スパムではない特定の送信者からの電子メールが自分のスパム隔離に送信されていることに気づくこともあります。これらの送信者からのメッセージが隔離されないようにするために、エンドユーザはそれらの送信者を自分のセーフリストに追加できます。

エンドユーザおよび管理者が行った変更はお互いに表示され、両者が変更できます。

関連項目

- [セーフリストとブロックリストのメッセージ処理 \(10 ページ\)](#)
- [レガシー Web インターフェイスでのセーフリストとブロックリストの有効化 \(11 ページ\)](#)
- [外部スパム隔離およびセーフリスト/ブロックリスト \(12 ページ\)](#)
- [セーフリストおよびブロックリストへの送信者とドメインの追加 \(管理者\) \(12 ページ\)](#)
- [セーフリストおよびブロックリストへのエンドユーザ アクセスについて \(19 ページ\)](#)
- [セーフリスト/ブロックリストのバックアップと復元 \(21 ページ\)](#)
- [セーフリストとブロックリストのトラブルシューティング \(22 ページ\)](#)

セーフリストとブロックリストのメッセージ処理

セーフリストまたはブロックリストに送信者を追加しても、アプライアンスではメッセージに対するウイルスのスクランや、内容に関連したメールポリシーの基準をメッセージが満たすかどうかの判定が行われます。受信者のセーフリストにメッセージの送信者が含まれていても、他のスクラン設定と結果によってはメッセージが配信されない場合があります。

セーフリストとブロックリストを有効にすると、アプライアンスは、アンチスパム スキャンの直前にセーフリスト/ブロックリスト データベースと照合してメッセージをスキャンします。アプライアンスがセーフリストまたはブロックリストのエントリに一致する送信者またはドメインを検出した場合、受信者が複数存在すると（かつ各受信者のセーフリスト/ブロックリスト設定が異なると）、そのメッセージは分裂します。たとえば、受信者 A と受信者 B の両方に送信されるメッセージがあるとします。受信者 A のセーフリストにはこの送信者のエントリがありますが、受信者 B のセーフリストおよびブロックリストにはエントリがありません。この場合、メッセージは 2 つのメッセージ ID で 2 つのメッセージに分割されます。受信者 A に送信されるメッセージは、セーフリストに一致していることが X-SLBL-Result-セーフリスト ヘッダーによってマークされ、アンチスパム スキャンをスキップします。一方、受信者 B 宛のメッセージは、アンチスパム スキャン エンジンによってスキャンされます。その後、どちらのメッセージもパイプライン（アンチウイルス スキャン、コンテンツ ポリシーなど）を続行し、設定されているすべての設定に従います。

メッセージの送信者またはドメインがブロックリストに含まれる場合の配信の動作は、セーフリスト/ブロックリスト機能を有効にするときに指定したブロックリストアクションによって決まります。セーフリストの配信の場合と同様に、セーフリスト/ブロックリスト設定の異なる複数の受信者が存在すると、そのメッセージは分裂します。分裂したメッセージのうちブロックリストに含まれるものは、ブロックリストアクション設定に応じて隔離されるかドロ

プされます。隔離を実行するようにブロックリストアクションが設定されている場合、そのメッセージはスキャンされ、最終的に隔離されます。削除するようにブロックリストアクションが設定されている場合、そのメッセージは、セーフリスト/ブロックリスト スキャンの直後にドロップされます。

セーフリストとブロックリストはスパム隔離内に保持されているため、配信の動作は、他のアンチスパム設定にも左右されます。たとえば、アンチスパムスキャンをスキップするようにホストアクセス テーブル (HAT) で「承認 (Accept)」メールフロー ポリシーを設定すると、そのリスナー上でメールを受信するユーザは、自分のセーフリストとブロックリストの設定がそのリスナー上で受信されたメールに適用されなくなります。同様に、一部のメッセージ受信者についてアンチスパム スキャンをスキップするメール フロー ポリシーを作成すると、それらの受信者は、自分のセーフリストとブロックリストの設定が適用されなくなります。

関連項目

- [レガシー Web インターフェイスでのセーフリストとブロックリストの有効化 \(11 ページ\)](#)
- [外部スパム隔離およびセーフリスト/ブロックリスト \(12 ページ\)](#)


セーフリストとブロックリストの有効化

- [レガシー Web インターフェイスでのセーフリストとブロックリストの有効化 \(11 ページ\)](#)

レガシーWebインターフェイスでのセーフリストとブロックリストの有効化

始める前に

- スпам隔離を有効にする必要があります。「[中央集中型スパム隔離の設定 \(2 ページ\)](#)」を参照してください。

-
- ステップ 1** (新しい Web インターフェイスのみ) セキュリティ管理アプライアンスで  をクリックして、レガシー Web インターフェイスをロードします。
 - ステップ 2** [管理アプライアンス (Management Appliance)] > [集約サービス (Centralized Services)] > [スパム隔離 (Spam Quarantine)] に移動します。
 - ステップ 3** [エンドユーザセーフリスト/ブロックリスト (End-User Safelist/Blocklist)] の下にある [設定の編集 (Edit Settings)] をクリックします。
 - ステップ 4** [エンドユーザセーフリスト/ブロックリスト機能を有効にする (Enable End User Safelist/Blocklist Feature)] を選択します。
 - ステップ 5** [ユーザごとの最大リスト項目数 (Maximum List Items Per User)] を指定します。

これは、各受信者のリストごとのアドレスまたはドメインの最大数です。ユーザごとのリストエントリ数を大きくすると、システムのパフォーマンスに悪影響を与えることがあります。

ステップ6 [更新頻度 (Update Frequency)] を選択します。

この値によって、外部スパム隔離を使用するEメールセキュリティアプライアンスのセーフリスト/ブロックリストを AsyncOS が更新する頻度が決まります。この設定の意味については、[外部スパム隔離およびセーフリスト/ブロックリスト \(12 ページ\)](#) で説明します。

ステップ7 変更を送信し、保存します。

外部スパム隔離およびセーフリスト/ブロックリスト

Eメールセキュリティアプライアンスは受信メールの処理時にセーフリストとブロックリスト内の送信者を評価するため、セキュリティ管理アプライアンスに保存されているセーフリストおよびブロックリストが受信メールに適用されるように、これらをEメールセキュリティアプライアンスに送信する必要があります。セキュリティ管理アプライアンスでセーフリスト/ブロックリスト機能を設定する際に、その更新頻度を設定します。

セーフリストおよびブロックリストへの送信者とドメインの追加（管理者）

スパム隔離のインターフェイスでセーフリストとブロックリストを管理します。

多数の受信者（組織のエンドユーザ）が特定の送信者またはドメインを許可リストまたはブロックリストに含めているかどうかを確認できます。

管理者は、各エンドユーザが表示および操作する同じエントリのスーパーセットを表示して操作します。

始める前に

- スパム隔離にアクセスできることを確認します。[スパム隔離へのアクセス（管理ユーザ）（34 ページ）](#) を参照してください。
- セーフリスト/ブロックリストへのアクセスを有効にします。[レガシー Web インターフェイスでのセーフリストとブロックリストの有効化（11 ページ）](#) を参照してください。
- （任意）このセクションの手順を使用してこれらのリストを作成する代わりに、セーフリスト/ブロックリストをインポートするには、[セーフリスト/ブロックリストのバックアップと復元（21 ページ）](#) で説明する手順を使用します。
- セーフリストとブロックリストのエントリの必須形式を把握します。[セーフリストエントリとブロックリストエントリの構文（18 ページ）](#) を参照してください。

ステップ1 （新しい Web インターフェイスのみ）セキュリティ管理アプリアンスで、[隔離（Quarantine）]>[スパム隔離（Spam Quarantine）]>[検索（Search）]をクリックします。

または

[電子メール（Email）]>[メッセージの隔離（Message Quarantine）]>[スパム隔離（Spam Quarantine）]を選択し、ページの右上隅にある[オプション（Options）]ドロップダウンメニューを選択します。

ステップ2 [セーフリスト（Safelist）]または[ブロックリスト（Blocklist）]を選択します。

ステップ3 （任意）送信者または受信者を検索します。

ステップ4 次の1つまたは複数の操作を実行します。

目的	操作手順
<p>1 人の受信者に対して複数の送信者を追加する</p>	<p>新しい Web インターフェイスで 1 人の受信者に複数の送信者を追加する場合</p> <ol style="list-style-type: none"> 1. [受信者 (Recipients)] タブを選択します。 2. +アイコンをクリックして、受信者のアドレスと送信者リストを追加します。 3. 受信者の電子メールアドレスを入力します。 4. 送信者の電子メールアドレスとドメインを入力します。 各エントリを別の行に入力するか、各エントリをカンマで区切ります。 5. <input checked="" type="checkbox"/> をクリックしてエントリを保存します。 <p>既存の送信者アドレスを変更するには、必要な受信者アドレスの横にあるチェックボックスをオンにして編集アイコンをクリックし、送信者のアドレスを変更してから <input checked="" type="checkbox"/> をクリックしてエントリを保存します。</p> <p>レガシー Web インターフェイスで 1 人の受信者に複数の送信者を追加する場合</p> <ol style="list-style-type: none"> 1. [表示方法：受信者 (View by: Recipient)] を選択します。 2. [追加 (Add)] をクリックするか、受信者の [編集 (Edit)] をクリックします。 3. 受信者の電子メールアドレスを入力または編集します。 4. 送信者の電子メールアドレスおよびドメインを入力します。 各エントリを別の行に入力するか、各エントリをカンマで区切ります。 5. [送信 (Submit)] をクリックします。

目的	操作手順
<p>1 人の送信者に対して複数の受信者を追加する</p>	<p>新しい Web インターフェイスで 1 人の送信者に複数の受信者を追加する場合</p> <ol style="list-style-type: none"> 1. [送信者 (Sender)] タブを選択します。 2. + をクリックして、送信者のアドレスと受信者リストを追加します。 3. 送信者のアドレスまたはドメインを入力します。 4. 受信者の電子メール アドレスを入力します。 <p>各エントリを別の行に入力するか、各エントリをカンマで区切ります。</p> <ol style="list-style-type: none"> 5. <input checked="" type="checkbox"/> をクリックしてエントリを保存します。 <p>既存の受信者アドレスを変更するには、必要な送信者アドレスの横にあるチェックボックスをオンにして編集アイコンをクリックし、送信者のアドレスを変更してから <input checked="" type="checkbox"/> をクリックしてエントリを保存します。</p> <p>レガシー Web インターフェイスで 1 人の送信者に複数の受信者を追加する場合</p> <ol style="list-style-type: none"> 1. [表示方法：送信者 (View by: Sender)] を選択します。 2. [追加 (Add)] をクリックするか、または送信者の [編集 (Edit)] をクリックします。 3. 送信者アドレスまたはドメインを入力または編集します。 4. 受信者の電子メール アドレスを入力します。 <p>各エントリを別の行に入力するか、各エントリをカンマで区切ります。</p> <ol style="list-style-type: none"> 5. [送信 (Submit)] をクリックします。

目的	操作手順
<p>受信者に関連付けられたすべての送信者を削除する</p>	<p>新しい Web インターフェイスで 1 人の受信者に関連付けられたすべての送信者を削除する場合</p> <ol style="list-style-type: none"> 1. 受信者または送信者のアドレスの横にあるチェックボックスをオンにしてエントリを選択します。 <p>すべてのエントリを選択し、削除することができます。</p> <ol style="list-style-type: none"> 2. ごみ箱アイコンをクリックしてテーブル行全体を削除できます。 <p>レガシー Web インターフェイスで 1 人の受信者に関連付けられたすべての送信者を削除する場合</p> <ol style="list-style-type: none"> 1. [表示方法（View by）] オプションを選択します。 2. ゴミ箱アイコンをクリックしてテーブル行全体を削除します。
<p>送信者に関連付けられたすべての受信者を削除する</p>	<p>新しい Web インターフェイスで 1 人の送信者に関連付けられたすべての受信者を削除する場合</p> <ol style="list-style-type: none"> 1. 受信者または送信者のアドレスの横にあるチェックボックスをオンにしてエントリを選択します。 <p>すべてのエントリを選択し、削除することができます。</p> <ol style="list-style-type: none"> 2. ごみ箱アイコンをクリックしてテーブル行全体を削除できます。 <p>レガシー Web インターフェイスで 1 人の送信者に関連付けられたすべての受信者を削除する場合</p> <ol style="list-style-type: none"> 1. [表示方法（View by）] オプションを選択します。 2. ゴミ箱アイコンをクリックしてテーブル行全体を削除します。

目的	操作手順
<p>受信者の個々の送信者を削除する</p>	<p>新しい Web インターフェイスで 1 人の受信者の個々の送信者を削除する場合</p> <ol style="list-style-type: none"> 1. 受信者または送信者のアドレスの横にあるチェックボックスをオンにしてエントリを選択します。 複数のエントリを選択、削除することができます。 2. 編集アイコンをクリックして、個々の受信者または送信者を変更します。 3. テキストボックスでエントリを追加または削除します。少なくとも 1 つはエントリを残す必要があります。 4. <input checked="" type="checkbox"/> をクリックしてエントリを保存します。 <p>レガシー Web インターフェイスで 1 人の受信者の個々の送信者を削除する場合</p> <ol style="list-style-type: none"> 1. [表示方法 (View by)] オプションを選択します。 2. 個々の受信者または送信者の [編集 (Edit)] をクリックします。 3. テキストボックスでエントリを追加または削除します。少なくとも 1 つはエントリを残す必要があります。 4. [送信 (Submit)] をクリックします。

目的	操作手順
送信者の個々の受信者を削除する	<p>新しい Web インターフェイスで 1 人の送信者の個々の受信者を削除する場合</p> <ol style="list-style-type: none"> 1. 受信者または送信者のアドレスの横にあるチェックボックスをオンにしてエントリを選択します。 複数のエントリを選択、削除することができます。 2. 編集アイコンをクリックして、個々の受信者または送信者を変更します。 3. テキストボックスでエントリを追加または削除します。少なくとも 1 つはエントリを残す必要があります。 4. <input checked="" type="checkbox"/> をクリックしてエントリを保存します。 <p>レガシー Web インターフェイスで 1 人の受信者の個々の送信者を削除する場合</p> <ol style="list-style-type: none"> 1. [表示方法 (View by)] オプションを選択します。 2. 個々の受信者または送信者の [編集 (Edit)] をクリックします。 3. テキストボックスでエントリを追加または削除します。少なくとも 1 つはエントリを残す必要があります。 4. [送信 (Submit)] をクリックします。

次のタスク

関連項目

- [セーフリスト エントリとブロックリスト エントリの構文 \(18 ページ\)](#)
- [すべてのセーフリストおよびブロックリストのクリア \(19 ページ\)](#)

セーフリスト エントリとブロックリスト エントリの構文

送信者を次の形式でセーフリストとブロックリストに追加できます。

- user@domain.com
- server.domain.com
- domain.com
- [10.1.1.0]
- [ipv6:2001:DB8:1::1]
- user@[1.2.3.4]

- user@[ipv6:2001:db8::1]

送信者アドレスやドメインなどの同一エントリを、セーフリストとブロックリストの両方に同時に追加することはできません。ただし、ドメインをセーフリストに追加し、そのドメインに所属する送信者の電子メールアドレスをブロックリストに追加すること(またはその逆)は可能です。両方のルールが適用されます。たとえば *example.com* がセーフリストに含まれている場合、*george@example.com* をブロックリストに追加することができます。この場合アプライアンスは、スパムとして処理される *george@example.com* からのメールを除いて、*example.com* からのすべてのメールをスパムのスキャンなしで配信します。

.domain.com のような構文を使用して、サブドメインの範囲を許可したり、ブロックしたりすることはできません。ただし、構文 *server.domain.com* を使用して特定のドメインをブロックすることは可能です。

すべてのセーフリストおよびブロックリストのクリア

すべての送信者と受信者を含む、セーフリストおよびブロックリストのすべてのエントリを削除する必要がある場合は、[セーフリスト/ブロックリストのバックアップと復元 \(21 ページ\)](#) の手順を使用してエントリなしでファイルをインポートします。

セーフリストおよびブロックリストへのエンドユーザアクセスについて

エンドユーザはスパム隔離から各自のセーフリストとブロックリストにアクセスします。スパムの隔離へのエンドユーザアクセスを設定するには、「[Web ブラウザからのスパム隔離へのエンドユーザアクセスの設定](#)」を参照してください。

必要に応じて、スパム隔離の URL と下記の手順をエンドユーザに提供してください。

関連項目

- [セーフリストへのエントリの追加 \(エンドユーザ\)](#)
- [ブロックリストへの送信者の追加 \(エンドユーザ\)](#)

セーフリストへのエントリの追加 (エンドユーザ)



(注) セーフリストに登録されている送信者からのメッセージの配信は、システムの他の設定によって異なります。[セーフリストとブロックリストのメッセージ処理 \(10 ページ\)](#) を参照してください。

エンドユーザは、次の2つの方法で送信者をセーフリストに追加できます。

- [隔離されたメッセージの送信者のセーフリストへの追加 \(20 ページ\)](#)
- [隔離されたメッセージのない送信者のセーフリストへの追加 \(20 ページ\)](#)

隔離されたメッセージの送信者のセーフリストへの追加

エンドユーザは、スパム隔離に送信されたメッセージの送信者をセーフリストに追加できます。

(新しい Web インターフェイスのみ) [リリースしてセーフリストに追加 (Release and Add to Safelist)] アイコンをクリックしてメッセージをリリースし、セーフリストに追加します。

または

ドロップダウンメニューから [リリースしてセーフリストに追加 (Release and Add to Safelist)] を選択します。

指定したメールのエンベロープ送信者と差出人ヘッダーが両方ともセーフリストに追加されます。解放されたメッセージは、それ以降の電子メールパイプライン内の作業キューの処理をスキップして、宛先キューへ直接進みます。

隔離されたメッセージのない送信者のセーフリストへの追加

ステップ 1 (新しい Web インターフェイスのみ) [セーフリスト (Safelist)] を選択します。

ステップ 2 (新しい Web インターフェイスのみ) 電子メールアドレスまたはドメインを入力します。ドメインと電子メールアドレスは、コンマで区切って複数入力できます。

ステップ 3 (新しい Web インターフェイスのみ) をクリックしてエントリを保存します。

ステップ 4 [スパム隔離 (Spam Quarantine)] ページにアクセスします。

- a) [モニタ (Monitor)] > [スパム隔離 (Spam Quarantine)] を選択します。
 - b) ページの右上隅にある [オプション (Options)] ドロップダウンメニューを選択します。
 - c) [セーフリスト (Safelist)] を選択します。
 - d) [セーフリスト (Safelist)] ダイアログボックスから、電子メールアドレスまたはドメインを入力します。ドメインと電子メールアドレスは、コンマで区切って複数入力できます。
 - e) [一覧に追加 (Add to List)] をクリックします。
-

ブロックリストへの送信者の追加 (エンドユーザ)

ブロックリストに登録されている送信者からのメッセージは、管理者が定義したセーフリスト/ブロックリストアクション設定に応じて、拒否または隔離されます。




(注) この手順でのみブロックリスト エントリを追加できます。

- ステップ 1** (新しい Web インターフェイスのみ) [ブロックリスト (Blocklist)] を選択し、[+] アイコンをクリックして、ブロックリストに追加するドメインまたは電子メールアドレスを入力します。ドメインと電子メールアドレスは、コンマで区切って複数入力できます。
- ステップ 2** (新しい Web インターフェイスのみ) をクリックしてエントリを保存します。
- ステップ 3** [スパム隔離 (Spam Quarantine)] ページにアクセスします。
- [モニタ (Monitor)] > [スパム隔離 (Spam Quarantine)] を選択します。
 - ページの右上にある [オプション (Options)] ドロップダウンメニューから [ブロックリスト (Blocklist)] を選択します。
 - ブロックリストに追加するドメインまたは電子メールアドレスを入力します。ドメインと電子メールアドレスは、コンマで区切って複数入力できます。
 - [一覧に追加 (Add to List)] をクリックします。

セーフリスト/ブロックリストのバックアップと復元

アプライアンスをアップグレードする場合、またはインストールウィザードを実行する場合、事前にセーフリスト/ブロックリスト データベースをバックアップする必要があります。セーフリスト/ブロックリストの情報は、アプライアンスの設定が格納されるメインの XML コンフィギュレーションファイルには含まれていません。

セーフリスト/ブロックリスト エントリは、セキュリティ管理アプライアンスの他のデータと共にバックアップすることもできます。[セキュリティ管理アプライアンスのデータのバックアップ](#)を参照してください。

- ステップ 1** (新しい Web インターフェイスのみ) セキュリティ管理アプライアンスで  をクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [設定ファイル (Configuration File)] を選択します。
- ステップ 3** [エンドユーザセーフリスト/ブロックリストデータベース(スパム隔離) (End-User Safelist/Blocklist Database (Spam Quarantine))] セクションまでスクロールします。

目的	操作手順
セーフリスト/ブロックリストをエクスポートする	.csv ファイルのパスおよびファイル名をメモし、必要に応じて変更します。 [すぐにバックアップ (Backup Now)] をクリックします。 アプライアンスは次の命名規則を使用して、アプライアンスの /configuration ディレクトリに .csv ファイルを保存します。 <i>slbl-<serial number>-<timestamp>.csv</i>

目的	操作手順
セーフリスト/ブロックリストをインポートする	<p>注意 このプロセスによって、すべてのユーザのセーフリストおよびブロックリストの既存のエントリがすべて上書きされます。</p> <p>[リストアするファイルを選択 (Select File to Restore)] をクリックします。</p> <p>configuration ディレクトリ内のファイルリストから目的のファイルを選択します。</p> <p>復元するセーフリスト/ブロックリストバックアップファイルを選択します。</p> <p>[復元 (Restore)] をクリックします。</p>

セーフリストとブロックリストのトラブルシューティング

セーフリストとブロックリストに関する問題をトラブルシューティングするために、ログファイルまたはシステムアラートを表示できます。

電子メールがセーフリスト/ブロックリスト設定によってブロックされると、そのアクションが ISQ_log ファイルまたはアンチスパム ログ ファイルに記録されます。セーフリストに含まれる電子メールは、セーフリストに一致していることが *X-SLBL-Result*-セーフリストヘッダーによってマークされます。ブロックリストに含まれる電子メールは、ブロックリストに一致していることが *X-SLBL-Result*-ブロックリストヘッダーによってマークされます。

アラートは、データベースが作成または更新されたり、データベースの変更またはセーフリスト/ブロックリストプロセスの実行においてエラーが発生したりすると送信されます。

アラートの詳細については、[アラートの管理](#)を参照してください。

ログファイルの詳細については、[ログ](#)を参照してください。

関連項目

- [セーフリストに登録されている送信者からのメッセージが配信されない](#) (22 ページ)

セーフリストに登録されている送信者からのメッセージが配信されない

問題

セーフリストに登録されている送信者からのメッセージが配信されませんでした。

解決方法

考えられる原因：

- マルウェアまたはコンテンツ違反のためメッセージがドロップされました。[セーフリストとブロックリストのメッセージ処理](#) (10 ページ) を参照してください。
- アプライアンスが複数あり、その送信者をセーフリストに最近追加した場合、メッセージが処理された時点ではセーフリスト/ブロックリストが同期されていなかった可能性があります。

ります。[外部スパム隔離およびセーフリスト/ブロックリスト \(12 ページ\)](#) を参照してください。

エンドユーザーのためのスパム管理機能の設定

目的	参照先
スパム管理機能へのエンドユーザー アクセスのさまざまな認証方式について、利点と制限事項を把握します。	スパム隔離へのエンドユーザーアクセスの設定 (26 ページ) およびサブセクション
エンドユーザーがブラウザから直接スパム隔離にアクセスすることを許可します。	スパム管理機能にアクセスするエンドユーザーの認証オプション (23 ページ)
メッセージがスパム隔離にルーティングされたときに、その宛先のユーザーに通知を送信します。 通知にはスパム隔離へのリンクを含めることができます。	エンドユーザーへの隔離されたメッセージに関する通知 (29 ページ)
ユーザーが、安全であると判断した送信者、およびスパムまたはその他の無用なメールを送信すると判断した送信者の電子メールアドレスとドメインを指定できるようにします。	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 (9 ページ)

関連項目

- [スパム管理機能にアクセスするエンドユーザーの認証オプション \(23 ページ\)](#)
- [Web ブラウザからのスパム隔離へのエンドユーザーアクセスの設定 \(26 ページ\)](#)
- [エンドユーザーへの隔離されたメッセージに関する通知 \(29 ページ\)](#)

スパム管理機能にアクセスするエンドユーザーの認証オプション



(注) メールボックス認証では、ユーザーが電子メールエイリアス宛てのメッセージを表示することはできません。

エンドユーザによるスパム隔離へのアクセスの場合	操作手順
Web ブラウザから直接アクセス、認証必須 および 通知内のリンク経由でアクセス、認証必須	<ol style="list-style-type: none"> <li data-bbox="787 331 1481 478">1. [エンドユーザ隔離アクセス (End User Quarantine Access)] 設定で、[LDAP]、[SAML 2.0] または [メールボックス (IMAP/POP) (Mailbox (IMAP/POP))] を選択します。 <li data-bbox="787 485 1481 625">2. [スパム通知 (Spam Notifications)] 設定で、[隔離へのアクセスに証明書なしのログインを有効にする (Enable login without credentials for quarantine access)] の選択を解除します。
Web ブラウザから直接アクセス、認証必須 および 通知内のリンク経由でアクセス、認証不要	<ol style="list-style-type: none"> <li data-bbox="787 653 1481 800">1. [エンドユーザ隔離アクセス (End User Quarantine Access)] 設定で、[LDAP]、[SAML 2.0] または [メールボックス (IMAP/POP) (Mailbox (IMAP/POP))] を選択します。 <li data-bbox="787 806 1481 947">2. [スパム通知 (Spam Notifications)] 設定で、[隔離へのアクセスに証明書なしのログインを有効にする (Enable login without credentials for quarantine access)] をオンにします。
通知内のリンク経由でのみアクセス、認証不要	[エンドユーザ隔離アクセス (End User Quarantine Access)] 設定で、認証方式として [なし (None)] を選択します。
アクセスなし	[エンドユーザ隔離アクセス (End User Quarantine Access)] 設定で、[エンドユーザの隔離へのアクセスを有効にする (Enable End-User Quarantine Access)] の選択を解除します。

関連項目

- [LDAP 認証プロセス \(24 ページ\)](#)
- [IMAP/POP 認証プロセス \(25 ページ\)](#)
- [SAML 2.0 認証プロセス \(26 ページ\)](#)
- [スパム隔離へのエンドユーザ アクセスの設定 \(26 ページ\)](#)
- [エンドユーザへの隔離されたメッセージに関する通知 \(29 ページ\)](#)
- [スパム隔離と連携させるための LDAP の設定](#)
- [セーフリストおよびブロックリストへのエンドユーザ アクセスについて \(19 ページ\)](#)

LDAP 認証プロセス

1. ユーザは、自分のユーザ名とパスワードを Web UI ログイン ページに入力します。
2. スパム隔離は、匿名検索を実行するように、または指定された「サーバログイン」DN とパスワードによる認証ユーザとして、指定された LDAP サーバに接続します。Active Directory の場合、一般に「グローバルカタログ ポート」(6000 番台) 上でサーバ接続を

確立する必要があり、検索を実行するために、スパム隔離がバインドできる低い特権LDAPユーザを作成する必要があります。

- 次に、スパム隔離は、指定された BaseDN とクエリ スtring を使用してユーザを検索します。ユーザの LDAP レコードが見つかったら、スパム隔離は、そのレコードの DN を抽出し、ユーザレコードの DN と最初にユーザが入力したパスワードを使用してディレクトリへのバインドを試みます。このパスワードチェックに成功すると、ユーザは正しく認証されます。しかしまだ、スパム隔離は、そのユーザに対してどのメールボックスの内容を表示するのか決定する必要があります。
- メッセージは、受信者のエンベロープ アドレスを使用してスパム隔離に保管されます。ユーザのパスワードが LDAP に対して検証された後、スパム隔離は、「プライマリ電子メール属性」を LDAP レコードから取得して、どのエンベロープ アドレスの隔離されたメッセージを表示する必要があるのか決定します。「プライマリ電子メール属性」には、電子メールアドレスが複数格納されている場合があります、これらのアドレスを使用して、隔離からどのエンベロープ アドレスが認証ユーザに対して表示される必要があるのか決定されます。

関連項目

- [スパム管理機能にアクセスするエンドユーザの認証オプション \(23 ページ\)](#)
- [LDAP との統合](#)

IMAP/POP 認証プロセス

- メールサーバ設定に応じて、ユーザは、自分のユーザ名 (joe) または電子メールアドレス (joe@example.com) と、パスワードを WebUI ログインページに入力します。ユーザに電子メールアドレスをフルに入力する必要があるのか、ユーザ名だけを入力すればよいのか知らせるために、ログイン ページメッセージを変更できます ([スパム隔離へのエンドユーザアクセスの設定 \(26 ページ\)](#) を参照)。
- スパム隔離は、IMAP サーバまたは POP サーバに接続し、入力されたログイン名 (ユーザ名または電子メールアドレス) とパスワードを使用して IMAP/POP サーバへのログインを試みます。パスワードが受け入れられると、そのユーザは認証されたと見なされ、スパム隔離はただちに IMAP/POP サーバからログアウトします。
- ユーザが認証された後、スパム隔離は、ユーザの電子メールアドレスに基づいて、そのユーザ宛の電子メールのリストを作成します。
 - スпам隔離の設定において、修飾のないユーザ名 (joe など) に追加するドメインを指定している場合は、このドメインを後ろに追加してできる完全修飾電子メールアドレスを使用して、隔離エリア内の一致するエンベロープが検索されます。
 - それ以外の場合、スパム隔離は、入力された電子メールアドレスを使用して、一致するエンベロープを検索します。

IMAP の詳細については、ワシントン大学の Web サイトを参照してください。

<http://www.washington.edu/imap/>

SAML 2.0 認証プロセス

『Cisco Content Security Management Appliance Guide』の「SSO Using SAML 2.0」セクションを参照してください。

Web ブラウザからのスパム隔離へのエンドユーザ アクセスの設定

- ステップ 1** スпам管理機能へのエンドユーザ アクセスのさまざまな認証方式について、利点と制限事項を把握します。
- ステップ 2** LDAP を使用してエンドユーザを認証する場合は、[システム管理 (System Administration)] > [LDAP] > [LDAPサーバプロファイル (LDAP Server Profile)] ページの [スパム隔離エンドユーザ認証クエリー (Spam Quarantine End-User Authentication Query)] 設定などで、LDAP サーバプロファイルを設定します。

例：

If you will authenticate end users using SAML 2.0 (SSO), configure the settings on the **System Administration > SAML** page.

[LDAP との統合](#) およびサブセクション

[SAML 2.0 による SSO](#)

- ステップ 3** スпам隔離へのエンドユーザ アクセスを設定します。
- [スパム隔離へのエンドユーザ アクセスの設定 \(26 ページ\)](#)
- ステップ 4** スпам隔離へのエンドユーザ アクセスの URL を決定します。
- [スパム隔離へのエンドユーザ アクセス用 URL の決定 \(28 ページ\)](#)

次のタスク

関連項目


- [スパム隔離へのエンドユーザ アクセスの設定 \(26 ページ\)](#)
- [スパム隔離へのエンドユーザ アクセス用 URL の決定 \(28 ページ\)](#)
- [エンドユーザに表示されるメッセージ \(29 ページ\)](#)

スパム隔離へのエンドユーザ アクセスの設定

管理ユーザは、エンドユーザアクセスがイネーブルにされているかどうかに関わらず、スパム隔離にアクセスできます。

始める前に

[スパム管理機能にアクセスするエンドユーザの認証オプション \(23 ページ\)](#) で要件を参照してください。

- ステップ 1** レガシーインターフェイスを使用している場合は、[管理アプライアンス (Management Appliance)] > [集約サービス (Centralized Services)] > [モニタ (Monitor)] > [スパム隔離 (Spam Quarantine)] > [設定の編集 (Edit Settings)] に移動し、[エンドユーザの隔離アクセス (End-User Quarantine Access)] へと下にスクロールします。新しい Web インターフェイスを使用している場合は、[セキュリティ管理アプライアンス (Security Management appliance)] に移動し、[サービスステータス (Service Status)] をクリックして  アイコンにマウスのカーソルを合わせて [エンドユーザの隔離設定の編集 (Edit End-User Quarantine Settings)] をクリックします。レガシーインターフェイスにリダイレクトされます。
- ステップ 2** [エンドユーザの隔離へのアクセスを有効にする (Enable End-User Quarantine Access)] を選択します。
- ステップ 3** エンドユーザが隔離されたメッセージを表示しようとしたときに、エンドユーザの認証に使用する方式を指定します。

選択オプション	追加情報
なし	このオプションを選択すると、追加の認証なしでスパム通知内のリンクを介してエンドユーザが隔離されたメッセージにアクセスできるようになります。
メールボックス (IMAP/POP)	<p>認証に LDAP ディレクトリを使用しないサイトの場合、隔離は、ユーザの電子メールアドレスとパスワードの正当性を、それらのユーザのメールボックスが保持されている標準ベースの IMAP または POP サーバに対して検証することもできます。</p> <p>スパム隔離にログインするとき、エンドユーザは自身の完全な電子メールアドレスとメールボックスのパスワードを入力します。</p> <p>POP サーバがバナー内で APOP サポートをアドバタイズしている場合、セキュリティ上の理由から (つまり、パスワードが平文で送信されるのを回避するために)、Cisco アプライアンスは APOP のみを使用します。一部またはすべてのユーザに対して APOP がサポートされていない場合は、APOP をアドバタイズしないように POP サーバを設定する必要があります。</p> <p>サーバで SSL を使用するように設定している場合は、SSL を選択します。ユーザがユーザ名だけを入力した場合に、電子メールアドレスを自動入力するために追加するドメインを指定できます。「権限のないユーザ名にドメインを追加 (Append Domain to Unqualified Usernames)」するには、ログインするユーザ用のエンベロープのドメインを入力します。</p>
LDAP	このトピックの「はじめる前に」で触れたセクションの説明に従って、LDAP を設定します。

選択オプション	追加情報
SAML 2.0	<p>スパム隔離用のシングル サインオンを有効にします。</p> <p>このオプションを使用する前に、[管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [SAML] ページのすべての設定が行われていることを確認します。『Cisco Content Security Management Appliance Guide』の「SSO Using SAML 2.0」のセクションを参照してください。</p>

ステップ 4 メッセージが解放される前に、メッセージ本文を表示するかどうかを指定します。

このチェックボックスをオンにすると、ユーザは、スパム隔離ページからメッセージ本文を表示できなくなります。この場合、隔離されたメッセージの本文を表示するには、そのメッセージを解放してから、ユーザのメールアプリケーション (Microsoft Outlook など) で表示する必要があります。この機能は、ポリシーおよび規制 (表示したすべての電子メールをアーカイブすることが要求されている場合など) へのコンプライアンスの目的で使用できます。

ステップ 5 変更を送信し、保存します。

次のタスク

(任意) ユーザがスパム隔離にアクセスしたときに表示されるページをカスタマイズします (まだ行っていない場合)。 [レガシー Web インターフェイスでのスパム隔離の有効化と設定 \(3 ページ\)](#) の設定の説明を参照してください。

スパム隔離へのエンドユーザ アクセス用 URL の決定

エンドユーザがスパム隔離に直接アクセスするために使用できる URL は、マシンのホスト名と、隔離が有効になっている IP インターフェイス上の設定 (HTTP/S とポート番号) から作成されます。たとえば、`HTTP://mail3.example.com:82` となります。

エンドユーザは、以下のいずれかの方法で、新しい Web インターフェイスのスパム検疫にアクセスできます。

- `trailblazerconfig CLI` コマンドが有効になっているときに、`https://example.com:<trailblazer-https-port>/euq-login` の URL を使用します。
ここで、`example.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` はアプライアンスで設定されている先駆者の HTTPS ポートです。
- `trailblazerconfig CLI` コマンドが無効になっているときに、`https://example.com:<https-port>/euq-login` の URL を使用します。
ここで、`example.com` はアプライアンスのホスト名で、`<https-port>` はアプライアンスで設定されている HTTPS ポートです。



- (注) ローカルおよび外部認証のユーザは、エンドユーザのスパム隔離ポータルにログインできません。

エンドユーザに表示されるメッセージ

通常、エンドユーザにはスパム隔離内にある自身のメッセージだけが表示されます。

アクセス方法（通知経由または Web ブラウザから直接）と認証方式（LDAP または IMAP/POP）によっては、スパム隔離内にある複数の電子メールアドレス宛のメールが表示される場合があります。

LDAP 認証を使用する場合、LDAP ディレクトリ内でプライマリ電子メール属性に複数の値が設定されていると、それらの値（アドレス）のすべてがユーザに関連付けられます。したがって、検疫エリア内には、LDAP ディレクトリでエンドユーザに関連付けられたすべての電子メールアドレス宛の検疫されたメッセージが存在します。

認証方式が IMAP/POP の場合、またはユーザが通知から直接隔離にアクセスした場合は、そのユーザの電子メールアドレス（または通知の送信先アドレス）宛のメッセージのみが隔離に表示されます。

メンバーになっているエイリアスに送信されたメッセージについては、[受信者の電子メールのメーリングリストエイリアスおよびスパム通知](#)（32 ページ）を参照してください。

関連項目

- [スパム隔離へのエンドユーザアクセスの設定](#)（26 ページ）
- [受信者の電子メールのメーリングリストエイリアスおよびスパム通知](#)（32 ページ）

エンドユーザへの隔離されたメッセージに関する通知

特定またはすべてのユーザに、スパム隔離内にスパムまたはその疑いのあるメッセージがあることを通知する電子メールを送信するように、システムを設定できます。

デフォルトでは、エンドユーザの隔離されたメッセージがスパム通知に表示されます。通知には、ユーザがスパム隔離内に隔離されたメッセージを表示できるリンクが含まれます。隔離されたメッセージを受信トレイに送るか、削除するかを決定できます。




- (注) クラスタ設定では、マシンレベルでのみ通知を受信するユーザを選択できます。

始める前に

- エンドユーザが通知に表示されるメッセージを管理するには、スパム隔離にアクセスする必要があります。[スパム隔離へのエンドユーザアクセスの設定](#)（26 ページ）を参照してください。

- 通知を使用してスパムを管理するための認証オプションを把握して実装します。 [スパム管理機能にアクセスするエンドユーザの認証オプション \(23 ページ\)](#) を参照してください。
- エンドユーザが複数のエイリアスで電子メールを受信する場合には、 [受信者の電子メールのメーリングリストエイリアスおよびスパム通知 \(32 ページ\)](#) を参照してください。

ステップ 1 レガシーインターフェイスを使用している場合は、[管理アプライアンス (Management Appliance)] > [集約サービス (Centralized Services)] > [スパム隔離 (Spam Quarantine)] > [設定の編集 (Edit Settings)] に移動し、[スパム通知 (Spam Notifications)] へと下にスクロールします。ただし、新しい Web インターフェイスを使用している場合は、[セキュリティ管理アプライアンス (Security Management appliance)] に移動し、[サービスステータス (Service Status)] をクリックして  アイコンの上にカーソルを合わせ、[スパム通知設定の編集 (Edit Spam Notification Settings)] をクリックします。レガシーインターフェイスにリダイレクトされます。

ステップ 2 [スパム通知を有効にする (Enable Spam Notification)] を選択します。

ステップ 3 通知の差出人アドレスを入力します。

ステップ 4 通知するエンドユーザを指定します。

ステップ 5 (任意) 通知の件名をカスタマイズします。

ステップ 6 (任意) 通知のタイトルをカスタマイズします。

ステップ 7 通知のデフォルト言語を選択します。

ステップ 8 エンドユーザ向けに隔離アクセスを設定します。

- ユーザが通知に記載されたリンクをクリックしてスパム隔離にアクセスしたときにそのユーザが自動的にログインされるようにするには、[クレデンシャルを使用せずにログインする (Login without credentials)] チェックボックスをオンにします。エンドユーザは、通知の [リリース (Release)] リンクをクリックするだけでメッセージをリリースできます。このオプションをオフにすると、エンドユーザは通知の [リリース (Release)] リンクをクリックしてメッセージをリリースすることはできなくなります。

このオプションは、メールボックス (IMAP/POP)、LDAP、または SAML 2.0 のいずれかのエンドユーザ認証方式を選択した場合にのみ表示されます。認証方式として [なし (None)] を選択した場合、エンドユーザはスパム通知内のリンクをクリックすると、自動的にスパム隔離にログインします。

- 通知内のリンクの有効期限 (日数) を設定します。0 ~ 365 の範囲内の数を入力してください。これらのリンクは、指定された期間後に自動的に期限切れになります。リンクを期限切れにしない場合は、0 を入力します。

(メールボックス (IMAP/POP)、LDAP、および SAML 2.0 の場合) このオプションは、[クレデンシャルを使用せずにログインする (Login without credentials)] チェックボックスをオンにした場合にのみ設定できます。

CLI で `spamdigestconfig` コマンドを使用して有効期限を設定することもできます。

ステップ 9 メッセージ本文をカスタマイズします。

- a) (任意) デフォルトのテキストおよび変数をカスタマイズします。

変数を挿入するには、挿入する位置にカーソルを置いて、右側のメッセージ変数リストで変数の名前をクリックします。または変数を入力します。

次のメッセージ変数は、特定のエンドユーザに対応した実際の値に展開されます。

- [新規メッセージ数 (New Message Count)] (%new_message_count%) : ユーザの最後のログイン以後の新しいメッセージの数。
 - [総メッセージ数 (Total Message Count)] (%total_message_count%) : スпам隔離内にあるこのユーザ宛のメッセージの数。
 - [メッセージ保存期間 (Days Until Message Expires)] (%days_until_expire%)
 - [隔離URL (Quarantine URL)] (%quarantine_url%) : 隔離にログインし、メッセージを表示するための URL。
 - [ユーザ名 (Username)] (%username%)
 - [新しいメッセージテーブル (New Message Table)] (%new_quarantine_messages%) : ユーザの新しい隔離メッセージのリスト。送信者、メッセージ件名、日付、およびメッセージをリリースするリンクを示します。ユーザは、メッセージ件名をクリックしてスパム隔離のメッセージを表示します。
 - [新しいメッセージテーブル (件名なし)] (%new_quarantine_messages_no_subject%) : [新しいメッセージテーブル (New Message Table)] と似ていますが、各メッセージの件名の場所には [メッセージの表示 (View Message)] リンクのみが表示されています。
- b) スпам通知内のすべての隔離メッセージを表示するためにリンクを表示するか非表示にするかを選択します。[通知メールのすべての隔離メッセージを表示するリンクを表示する (Show link to show all Quaranted messages in Notification Mails)] で、要件に応じて [はい (Yes)] または [いいえ (No)] を選択します

(メールボックス (IMAP / POP) 、LDAP、および SAML 2.0 の場合) 。このオプションは、[[クレデンシャルを使用せずにログインする (Login without credentials)] チェックボックス ([隔離へのアクセス (Quarantine Access)] の下) をオンにした場合にのみ表示されます。

[はい (Yes)] を選択した場合は、スパム隔離にアクセスする前にエンドユーザを強制的に認証できます。[チャレンジアクセス (Challenge Access)] をオンにします。このオプションは、エンドユーザ認証方式として [なし (None)] を選択した場合は使用できません。

CLIで **spamdigestconfig** コマンドを使用して、リンクを表示または非表示にすることもできます。

- c) [メッセージのプレビュー (Preview Message)] をクリックして、メッセージの内容を確認します。

ステップ 10 メッセージ形式 (HTML、テキスト、または HTML/テキスト) を選択します。

ステップ 11 バウンスされた通知の送信先のアドレスを指定します。

ステップ 12 (任意) [統合されたメッセージは同じLDAPユーザの違うアドレスに送信されます (Consolidate messages sent to the same LDAP user at different addresses)] を選択します。

ステップ 13 通知スケジュールを設定します。

ステップ 14 変更を送信し、保存します。

次のタスク

これらの通知を確実に受信できるように、エンドユーザにスパム隔離からの通知電子メールの差出人アドレスを各自のメールアプリケーション（Microsoft Outlook、Mozilla Thunderbird など）の迷惑メール設定にある「許可リスト」に追加することを推奨してください。

関連項目

- [受信者の電子メールのメーリングリストエイリアスおよびスパム通知](#) (32 ページ)
- [通知のテスト](#) (33 ページ)
- [スパム通知のトラブルシューティング](#) (33 ページ)

受信者の電子メールのメーリングリストエイリアスおよびスパム通知

電子メールが隔離されている各エンベロープ受信者（メーリングリストおよびその他のエイリアスを含む）に通知を送信できます。メーリングリストごとに1つの要約を受信します。メーリングリストに通知を送信すると、リストの購読者全員に通知が届きます。複数の電子メールエイリアスに属するユーザ、通知を受信するLDAPグループに属するユーザ、または複数の電子メールアドレスを使用するユーザは、複数のスパム通知を受信する場合があります。次の表に、ユーザが複数の通知を受け取る状況の例を示します。

表 1: アドレス/エイリアスに応じた通知数

ユーザ (User)	電子メール アドレス	エイリアス	通知
Sam	sam@example.com	—	1
Mary	mary@example.com	dev@example.com qa@example.com pm@example.com	4
Joe	joe@example.com、 admin@example.com	hr@example.com	3

LDAP 認証を使用する場合、メーリングリストエイリアスに通知を送信しないように選択することができます。または、メーリングリストエイリアスにスパム通知を送信することを選択した場合、複数の通知が送信されないようにすることができます。[スパム隔離のエイリアス統合クエリ](#)を参照してください。

アプライアンスが電子メール通知にスパム隔離のエイリアス統合クエリを使用していない限り、通知内のリンクをクリックしてスパム隔離にアクセスしたユーザに、そのエンドユーザが所有する他のエイリアス宛の隔離対象メッセージは表示されません。アプライアンスで処理した後に展開される配布リストに通知が送信された場合、複数の受信者がそのリストの同じ隔離にアクセスできます。

つまり、各メーリングリストの購読者は、全員が同じ通知を受信することになり、その検疫にログインしてメッセージを解放したり、削除したりできます。この場合、エンドユーザが隔離にアクセスして、通知に示されたメッセージを表示しようとしても、それらのメッセージは他のユーザによってすでに削除されている可能性もあります。



(注) LDAPを使用していない場合で、エンドユーザが複数の電子メール通知を受信することがないようにする必要がある場合は、通知をディセーブルにすることを検討します。この場合、代わりとして、エンドユーザが検疫に直接アクセスできるようにし、LDAPまたはPOP/IMAPで認証します。

通知のテスト

テスト用のメールポリシーを設定し、単一のユーザに対してのみスパムを隔離することで通知をテストできます。その後、スパム隔離の通知設定で、[スパム通知を有効にする (Enable Spam Notification)] チェックボックスをオンにし、[エンドユーザの隔離へのアクセスを有効にする (Enable End-User Quarantine Access)] チェックボックスをオフにします。これにより、[バウンスされたメッセージの送信先 (Deliver Bounced Messages To)] フィールドに設定された管理者だけが、隔離内の新しいスパムについて通知されます。

スパム通知のトラブルシューティング

関連項目

- [ユーザが複数の通知を受信する \(33 ページ\)](#)
- [受信者が通知を受信しない \(33 ページ\)](#)
- [ユーザが複数の通知を受信する \(33 ページ\)](#)
- [受信者が通知を受信しない \(33 ページ\)](#)

ユーザが複数の通知を受信する

問題

ユーザが1つのメッセージに対して複数のスパム通知を受信します。

解決方法

考えられる原因：

- ユーザが複数の電子メールアドレスを所有し、スパムメッセージがその内の2つ以上のアドレスに送信されました。
- ユーザが、スパムメッセージを受信した1つ以上の電子メールエイリアスのメンバーです。重複を最小限にするための詳細については、[受信者の電子メールのメーリングリストエイリアスおよびスパム通知 \(32 ページ\)](#) を参照してください。

受信者が通知を受信しない

問題

受信者にスパム通知が届きません。

解決方法

- スпам受信者ではなく [バウンスメッセージの送信先： (Deliver Bounce Messages To:)] のアドレスに通知が送信される場合は、スパム通知が有効になっていても、スパム隔離へのアクセスが有効になっていないことを意味します。 [スパム管理機能にアクセスするエンドユーザの認証オプション \(23 ページ\)](#) を参照してください。
- ユーザに各自の電子メールクライアントの迷惑メール設定を確認してもらいます。
- [レガシー Web インターフェイスでのスパム隔離の有効化と設定 \(3 ページ\)](#) で [次を使用してメッセージを配信 (Deliver Messages Via)] に指定したアプライアンスまたはサーバに問題がないかを確認します。

スパム隔離内のメッセージの管理

ここでは、ローカルまたは外部のスパム隔離内にあるメッセージの操作方法について説明します。

管理ユーザはスパム隔離内のすべてのメッセージを表示および管理できます。

関連項目

- [スパム隔離へのアクセス \(管理ユーザ\) \(34 ページ\)](#)
- [スパム隔離内でのメッセージの検索 \(35 ページ\)](#)
- [スパム隔離内のメッセージの表示 \(35 ページ\)](#)
- [スパム隔離内のメッセージの配信 \(36 ページ\)](#)
- [スパム隔離からのメッセージの削除 \(36 ページ\)](#)

スパム隔離へのアクセス (管理ユーザ)

管理ユーザはスパム隔離内のすべてのメッセージを表示および管理できます。

スパム隔離へのアクセス (管理ユーザ)

管理ユーザはスパム隔離内のすべてのメッセージを表示および管理できます。

ステップ 1 (新しい Web インターフェイスのみ) セキュリティ管理アプライアンスで、[隔離 (Quarantine)] > [スパム隔離 (Spam Quarantine)] > [検索 (Search)] を選択します。

ステップ 2 [メール (Email)] > [メッセージの隔離 (Message Quarantine)] > [スパム隔離 (Spam Quarantine)] を選択し、[スパム隔離 (Spam Quarantine)] リンクをクリックします。

スパム隔離が別のブラウザ ウィンドウで開きます。

スパム隔離内でのメッセージの検索

ステップ 1 エンベロープ受信者を指定します。

(注) アドレスの一部を入力できます。

ステップ 2 入力した受信者に検索結果が厳密に一致する必要があるか、あるいは入力した値が検索結果のアドレスの一部、先頭、または末尾のいずれと一致する必要があるかを選択します。

ステップ 3 検索の対象期間を入力します。カレンダー アイコンをクリックして、日付を選択します。

ステップ 4 差出人アドレスを指定し、入力した値が検索結果のアドレスの一部、全体、先頭、または末尾のいずれと一致する必要があるかを選択します。

ステップ 5 [検索 (Search)]をクリックします。検索基準に一致するメッセージがページの[検索 (Search)]セクションの下に表示されます。

次のタスク

関連項目

[大量メッセージの検索 \(35 ページ\)](#)

大量メッセージの検索

スパム隔離内に大量のメッセージが収集されている場合、および検索条件が絞り込まれていない場合、クエリーの結果が返されるまでに非常に長い時間がかかる可能性があり、場合によってはタイムアウトします。

その場合、検索を再実行するかどうか確認されます。大量の検索が同時に複数実行されると、パフォーマンスに悪影響を与える可能性があることに注意してください。

スパム隔離内のメッセージの表示

メッセージのリストにより、スパム隔離内のメッセージが表示されます。一度に表示されるメッセージの件数を選択できます。列見出しをクリックすることにより、表示をソートできます。同じ列を再びクリックすると、逆順にソートされます。

メッセージの件名をクリックしてメッセージを表示します。これには、本文とヘッダーが含まれます。メッセージは、[メッセージの詳細 (Message Details)]ページに表示されます。メッセージの最初の 20 KB が表示されます。メッセージがそれよりも長い場合、表示は 20 KB で打ち切れ、メッセージの最後にあるリンクからメッセージをダウンロードできます。

[メッセージの詳細 (Message Details)] ページから、メッセージを削除したり ([削除 (Delete)] を選択)、[リリース (Release)] を選択してメッセージを解放したりできます。メッセージを解放すると、そのメッセージは配信されます。

メッセージについてさらに詳細な情報を表示するには、[メッセージトラッキング (Message Tracking)] リンクをクリックします。

次の点に注意してください。

- **添付ファイルを含むメッセージの表示**

添付ファイルを含むメッセージを表示すると、メッセージの本文が表示された後、添付ファイルのリストが続いて表示されます。

新しい Web インターフェイスでは、メッセージに添付ファイルが含まれている場合、メッセージの [添付ファイル (Attachment)] セクションに添付ファイルの詳細が表示されません。

- **HTML メッセージの表示**

スパム隔離では、HTML ベースのメッセージは近似で表示されます。画像は表示されません。

- **エンコーディングされたメッセージの表示**

Base64 でエンコーディングされたメッセージは、復号化されてから表示されます。

スパム隔離内のメッセージの配信

メッセージをリリースして配信するには、リリースする1つまたは複数のメッセージの隣にあるチェックボックスをクリックし、ドロップダウンメニューから [リリース (Release)] を選択します。その後、[送信 (Submit)] をクリックします。

ページに現在表示されているすべてのメッセージを自動で選択するには、見出し行にあるチェックボックスをクリックします。

リリースされたメッセージは、それ以降の電子メールパイプライン内の作業キューの処理をスキップして、宛先キューへ直接進みます。

スパム隔離からのメッセージの削除

スパム隔離では、メッセージが一定時間後に自動で削除されるように設定できます。また、スパム隔離が最大サイズに達したら、古いものから順にメッセージが自動で削除されるように設定することもできます。スパム隔離からメッセージを手動で削除することも可能です。

個別のメッセージを削除するには、削除するメッセージの隣にあるチェックボックスをクリックし、ドロップダウンメニューから [削除 (Delete)] を選択します。その後、[送信 (Submit)] をクリックします。ページに現在表示されているすべてのメッセージを自動で選択するには、見出し行にあるチェックボックスをクリックします。

スパム隔離内のすべてのメッセージを削除するには、その隔離を無効にし（[外部スパム隔離の無効化について（37 ページ）](#)）を参照）、[すべてのメッセージを削除（Delete All Messages）] リンクをクリックします。リンクの末尾にある括弧内の数字は、スパム隔離内のメッセージの件数です。

スパム隔離のディスク領域

隔離に使用できるディスク領域は、アプライアンス モデルによって異なります。[ディスク領域、クォータ、および使用状況の表示](#)を参照してください。

デフォルトでは、スパム隔離内のメッセージは一定期間後に自動的に削除されます。検疫エリアが満杯になった場合は、古いスパムから削除されます。この設定を変更するには、[レガシー Web インターフェイスでのスパム隔離の有効化と設定（3 ページ）](#)を参照してください。

関連項目

外部スパム隔離の無効化について

スパム隔離をディセーブルにする場合は、次を参照してください。

- ディセーブルになっているスパム隔離内にメッセージが存在する場合は、すべてのメッセージの削除を選択できます。
- スпамまたはその疑いのあるメッセージを隔離するように設定されたメールポリシーは、メッセージを配信するように設定が変更されます。Eメールセキュリティアプライアンスでメールポリシーの調整が必要になる場合があります。
- 外部スパム隔離を完全にディセーブルにするには、Eメールセキュリティアプライアンスとセキュリティ管理アプライアンスの両方でディセーブルにします。

Eメールセキュリティアプライアンスのみで外部スパム隔離をディセーブルにしても、外部隔離またはそのメッセージとデータは削除されません。

スパム隔離機能のトラブルシューティング

- [セーフリストとブロックリストのトラブルシューティング（22 ページ）](#)
- [スパム通知のトラブルシューティング（33 ページ）](#)

