CHAPTER 7

Cisco IronPort スパム隔離の管理

Cisco IronPort スパム隔離について

Cisco IronPort スパム隔離では、組織内の電子メール ユーザに対するスパム メッセージやスパムであると疑われるメッセージを捕捉します。スパム隔離は、「誤検出」（正規の電子メールがスパムとして検出または削除されること）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。この機能により、エンド ユーザおよび管理者は、スパムとフラグ付けされたメッセージを確認してから最終的な決定を下すことができるようになります。さらに、セーフリスト/ブロックリスト機能をイネーブルにすると、どのようなメッセージをスパムとしてマークするかをエンド ユーザ（電子メール ユーザ）が制御できるようになります。

（注） ポリシー、ウイルス、アウトブレイク隔離は、スパム隔離とは異なります。詳細については、使用する電子メール セキュリティ アプライアンスのマニュアルおよび第 8 章「集約ポリシー、ウイルス、およびアウトブレイク隔離」を参照してください。

ローカルの Cisco IronPort スパム隔離は、電子メール セキュリティ ゲートウェイ アプライアンスに常駐します。通常はシスコのコンテンツセキュリティ管理アプライアンスですが、別のコンテンツ アプライアンスにある*外部の* Cisco IronPort スパム隔離エリアに送信されるメッセージを使用できます。

（注） Cisco IronPort スパム隔離へのエンド ユーザのアクセスは、指定したユーザまたはユーザ グループに対してのみ実装できます。また、最初にエンド ユーザ アクセスを実装した後で、エンド ユーザが隔離内のメッセージを表示および解放することがほとんどない場合は、アクセスをディセーブルにできます。

また、スパムおよびその疑いのあるメッセージが隔離されたことをエンド ユーザに電子メールで通知するように、AsyncOS を設定することもできます。通知には、そのユーザ向けに現在 Cisco IronPort スパム隔離で捕捉されているメッセージの要約が記述されています。ユーザはこのメッセージを確認して、電子メールの受信ボックスに配信するか、削除するかを判断できます。また、ユーザは隔離された

メッセージ全体を検索することができます。スパム隔離には通知メッセージからアクセスすることも、Web ブラウザを使用して直接アクセスすることもできます。（スパム隔離にエンド ユーザが直接アクセスするには、認証が必要です）。詳細については、「エンド ユーザ隔離へのアクセスの設定」（P.7-9）を参照してください）。

デフォルトでは、Cisco IronPort スパム隔離は自己メンテナンス型になっています。古いメッセージによって隔離領域がすべて消費されることを避けるために、AsyncOS は Cisco IronPort スパム隔離から定期的にメールを削除します。

管理者レベルのすべてのユーザ（デフォルトの admin ユーザなど）は、Cisco IronPort スパム隔離にアクセスし、変更を行うことができます。AsyncOS オペレータ ユーザ、およびカスタム ロールによってスパム隔離へのアクセス権が割り当てられているユーザは、隔離コンテンツの表示および管理ができますが、隔離設定の変更はできません。Cisco IronPort スパム隔離へのエンド ユーザ アクセスがイネーブルになっている場合、メールのエンド ユーザは、隔離領域にある自分のメッセージにアクセスできます。

中央集中型スパム隔離の設定

スパム隔離を中央集中型にする前に、使用している電子メール セキュリティ アプライアンスでローカルのスパム隔離を設定し、動作をテストする必要があります。

アクティブなスパム隔離を電子メール セキュリティ アプライアンスからセキュリティ管理アプライアンスへ移行するには、次の作業を順番に行ってください。

- 「必要な IP アドレスの特定」（P.7-2）
- 「セキュリティ管理アプライアンスでの Cisco IronPort スパム隔離の設定」（P.7-2）
- 「セキュリティ管理アプライアンスでのインターフェイスの設定」（P.7-4）
- 「中央集中型スパム隔離のための電子メール セキュリティ アプライアンスの設定」（P.7-5）
- 「管理対象の各電子メール 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」（P.7-7）

必要な IP アドレスの特定

「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」（P.7-4）の手順で使用する 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 Data 2 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、付録 B「ネットワークと IP アドレスの割り当て」を参照してください。

セキュリティ管理アプライアンスでの Cisco IronPort スパム隔離の設定

手順

ステップ 1　セキュリティ管理アプライアンスで、[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）] を選択します。

ステップ 2　システム セットアップ ウィザードの実行後、Cisco IronPort スパム隔離を初めてイネーブルにする場合は、次の手順を実行します。

a.　[有効（Enable）] をクリックします。

b.　エンド ユーザ ライセンス契約書を確認して、[承認（Accept）] をクリックします。

ステップ 3　既存の設定を編集する場合は、[Cisco IronPort スパム隔離の設定（Cisco IronPort Spam Quarantine Settings）] セクションで [設定を編集（Edit Settings）] をクリックします。

ステップ 4　[隔離 IP インターフェイス（Quarantine IP Interface）] セクションで、ドロップダウン リストからスパム隔離用の適切な IP インターフェイスとポートを指定します。

デフォルトでは、スパム隔離で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。

電子メール 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。

ステップ 5　[送信メッセージ（Deliver Messages Via）] セクションで、対応するテキスト フィールドに、メールを配送するためのプライマリ ルートと代替用ルートを入力します。

セキュリティ管理アプライアンスからメッセージを直接送信することはしないため、発信する隔離関係の電子メール（スパム隔離から送信されるスパム通知やメッセージなど）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送する必要があります。

これらのメッセージは、SMTP またはグループウェア サーバを使用して送信できます。また、電子メール 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 Data2 インターフェイス）を指定することもできます。

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。

電子メール セキュリティ アプライアンスが複数台ある場合は、管理対象の任意の電子メール 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。

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。

ステップ 6　[次の日数の経過後に削除（Schedule Delete After）] セクションで、メッセージを削除する前に保持する日数を指定します。

または、[削除日を決めない（Do not schedule a delete）] オプション ボタンを選択して、スケジュールされた削除をディセーブルにします。削除をスケジュールするよう、隔離を設定することを推奨します。隔離によってキャパシティがいっぱいになると、最も古いメッセージから削除されます。

ステップ 7　[デフォルト言語（Default Language）] セクションで、デフォルト言語を指定します。

これは、エンド ユーザが Cisco IronPort スパム隔離にアクセスしたときに表示される言語です。

ステップ 8　（任意）[メッセージのリリース時に Cisco IronPort に通知（Notify Cisco IronPort upon Message Release）] で、解放されたメッセージのコピーを分析のために Cisco IronPort に送信する機能のチェックボックスをオンにします。

解放されたメッセージを分析のために送信するよう、隔離を設定することを推奨します。

ステップ 9　（任意）[スパム隔離のアピアランス（Spam Quarantine Appearance）] セクションで、エンド ユーザが隔離結果を表示するときに表示されるページをカスタマイズします。

次のオプションがあります。

- 現在のロゴを使用（Use Current logo）
- Cisco IronPort スパム隔離のロゴを使用（Use Cisco IronPort Spam Quarantine logo）
- カスタムロゴをアップロードする（Upload Custom logo）

[カスタムロゴをアップロードする（Upload Custom logo）] を選択すると、隔離されたメッセージを表示するためにユーザがログインしたときに、[Cisco IronPort スパム隔離（Cisco IronPort Spam Quarantine）] ページの上部にロゴが表示されます。このロゴは、最大で 550 x 50 ピクセルの .jpg、.gif、または .png ファイルにする必要があります。ロゴ ファイルがない場合、デフォルトの Cisco IronPort スパム隔離のロゴが使用されます。

ステップ 10　（任意）[ログイン メッセージ（Login Page Message）] テキスト フィールドに、ログイン ページのメッセージを入力します。このメッセージは、エンド ユーザに対して隔離へのログイン プロンプトを表示するときに表示されます。

ステップ 11　オプションで、Cisco IronPort スパム隔離を表示する権限を持つユーザのリストを変更します。詳細については、「Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定」（P.7-8）を参照してください。

ステップ 12　オプションで、エンド ユーザのアクセス、およびスパム通知を設定します。詳細については、「エンド ユーザのためのスパム管理機能の設定」（P.7-9）を参照してください。

ステップ 13　変更を送信し、保存します。

セキュリティ管理アプライアンスでの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、隔離に関係するメッセージ（通知や解放された電子メールなど）を 電子メール 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。

手順

ステップ 1　この手順は、「IP インターフェイスの設定」（P.A-2）の説明と併せて実行してください。

ステップ 2　セキュリティ管理アプライアンスで、[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　[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
- イーサネット ポート

  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、[送信メッセージ（Deliver Messages Via）] セクションでプライマリ サーバに指定した電子メール 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

  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
- ホスト名

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。

スパム隔離にアクセスするための IP アドレスの設定

管理者またはエンド ユーザがスパム隔離にアクセスするときには、専用のブラウザ ウィンドウが開きます。

手順

ステップ 1　セキュリティ管理アプライアンスで、[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 2　**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 3　[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。

- [HTTP] または [HTTPS]、あるいはその両方を選択し、ポートを指定します。
- 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。

  たとえば、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表示したくない場合には、代わりのホスト名を指定できます。

  ここに入力した URL や IP アドレスが、使用している DNS サーバで解決できることを確認してください。

ステップ 4　変更を送信し、保存します。

中央集中型スパム隔離のための電子メール セキュリティ アプライアンスの設定

セキュリティ管理アプライアンスで中央集中型の Cisco IronPort スパム隔離サービスを使用するには、電子メール セキュリティ アプライアンスでスパム隔離の設定を一部変更する必要があります。

操作内容	参照先
電子メール セキュリティ アプライアンスでスパム隔離が正しく動作していることを確認します。 何らかの問題がある場合は、スパム隔離を中央集中型にする前に解決します。	—
セキュリティ管理アプライアンスを外部スパム隔離として使用するよう、電子メール セキュリティ アプライアンスをイネーブル化および設定します。	「中央集中型スパム隔離のための電子メール セキュリティ アプライアンスの設定」（P.7-6）

操作内容	参照先
電子メール セキュリティ アプライアンス でローカルのスパム隔離をディセーブルにします。	ご使用の電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Disabling the Local Spam Quarantine」。 この変更によって生じたメール ポリシーを調整するための警告は無視します。メール ポリシーで外部スパム隔離を使用するようになります。
電子メール セキュリティ アプライアンスで既存のローカルのスパム隔離メッセージを管理する方法を確認します。	ご使用の電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Migrating from a Local Spam Quarantine to an External Quarantine」。

中央集中型スパム隔離のための電子メール セキュリティ アプライアンスの設定

電子メール セキュリティ アプライアンスでセキュリティ管理アプライアンスの Cisco IronPort スパム隔離を使用するには、電子メール セキュリティ アプライアンスの外部隔離を設定する必要があります。

（注） これまで、電子メール セキュリティ アプライアンスに別の外部スパム隔離を設定していた場合は、まず、その外部スパム隔離設定をディセーブルにする必要があります。

外部隔離を設定するには、次の手順を**すべての** 電子メール セキュリティ アプライアンスで実行する必要があります。

手順

ステップ 1　電子メール セキュリティ アプライアンスで、[セキュリティ サービス（Security Services）] > [外部スパム隔離（External Spam Quarantine）] を選択します。

ステップ 2　[設定（Configure）] をクリックします。

ステップ 3　チェックボックスを選択して、外部スパム隔離をイネーブルにします。

ステップ 4　Cisco IronPort スパム隔離の名前を入力します。隔離領域があるセキュリティ管理アプライアンスの名前を入力することもできます。

ステップ 5　セキュリティ管理アプライアンスの正しいインターフェイスの IP アドレスを入力します。

通常は管理インターフェイスのアドレスになります。具体的には、[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）] ページにある [隔離 IP インターフェイス（Quarantine IP Interface）] 設定で、セキュリティ管理アプライアンスに指定したインターフェイスに割り当てた IP アドレスです。

指定したインターフェイスの IP アドレスを表示するには、セキュリティ管理アプライアンスで、[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）] を選択して、インターフェイス名をクリックしてください。

ステップ 6　スパムおよびその疑いのあるメッセージの配信に使用するポート番号を入力します。デフォルトは 6025 です。このポート番号は、[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）] ページで入力した隔離ポート番号と同じである必要があります。

ステップ 7　簡単にするために、セーフリスト/ブロックリスト機能は後で設定します。全体の説明と詳細については、「エンド ユーザのセーフリスト/ブロックリスト機能の設定と管理」（P.7-12）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。

ステップ 9　ローカルのスパム隔離をディセーブルにします。ご使用の電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Disabling the Local Spam Quarantine」を参照してください。

この変更によって生じたメール ポリシーを調整するための警告は無視します。メール ポリシーで外部スパム隔離を使用するようになります。

ステップ 10　管理対象の電子メール セキュリティ アプライアンスに対して、この手順を繰り返します。

管理対象の各電子メール 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。

手順

ステップ 1　セキュリティ管理アプライアンスで、[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 2　このページのリストに、すでに電子メール 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。

a.　電子メール セキュリティ アプライアンスの名前をクリックします。

b.　[スパム隔離（Spam Quarantine）] サービスを選択します。

ステップ 3　電子メール 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。

a.　[メール アプライアンスの追加（Add Email Appliance）] をクリックします。

b.　[アプライアンス名および IP アドレス（Appliance Name and IP Address）] テキスト フィールドに、Cisco IronPort 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）] テキスト 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、すぐに IP アドレスに解決されます。

c.　Spam Quarantine サービスが事前に選択されています。

d.　[接続の確立（Establish Connection）] をクリックします。

e.　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、セキュリティ管理アプライアンスには保存されません。

f. [成功（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。

g. [テスト接続（Test Connection）] をクリックします。

h. テーブルの上のテスト結果を確認します。

ステップ 4　[送信（Submit）] をクリックします。

ステップ 5　スパム隔離をイネーブルにする電子メール 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。

ステップ 6　変更を保存します。

Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定

この項の手順を実行すると、Operator、Read-Only Operator、Help Desk のロール、または Guest ロール、およびスパム隔離にアクセスできるカスタム ユーザ ロールを持つ管理者ユーザが、Cisco IronPort スパム隔離でメッセージを管理できるようになります。

デフォルトの admin ユーザ、Email Administrator ユーザを含む Administrator レベルのユーザは、常にスパム隔離にアクセスできるので、この手順を使用してスパム隔離機能に関連付ける必要はありません。

（注）　管理者レベル以外のユーザはスパム隔離のメッセージにアクセスできますが、隔離の設定を編集することはできません。管理者レベルのユーザは、メッセージにアクセスし、設定を編集することができます。

完全な管理者権限を持っていない管理者ユーザがスパム隔離のメッセージを管理できるようにするには、次の手順を実行してください。

手順

ステップ 1　ユーザを作成し、そのユーザにスパム隔離へのアクセス権があるユーザ ロールを割り当てる必要があります。詳細については、「管理タスクの分散について」（P.13-1）を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[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）] を選択します。

ステップ 3　[スパム隔離設定（Spam Quarantine Settings）] セクションで、[有効（Enable）] または [設定を編集（Edit Settings）] をクリックします。

ステップ 4　[スパム隔離設定（Spam Quarantine Settings）] セクションの [管理ユーザ（Administrative Users）] 領域で、[ローカル ユーザ（Local Users）]、[外部認証ユーザ（Externally Authenticated Users）]、または [カスタム ユーザ ロール（Custom User Roles）] の選択リンクをクリックします。

ステップ 5　スパム隔離のメッセージを表示および管理できるアクセス権を付与するユーザを選択します。

ステップ 6　[OK] をクリックします。

ステップ 7　必要な場合、このセクションの [管理ユーザ（Administrative Users）] にリストされているその他のタイプ（[ローカル ユーザ（Local Users）]、[外部認証ユーザ（Externally Authenticated Users）]、または [カスタム ユーザ ロール（Custom User Roles）]）について繰り返します。

ステップ 8　変更を送信し、保存します。

エンドユーザのためのスパム管理機能の設定

（注）　追加設定はいずれか 1 つだけ設定でき、それ以外は設定できません。たとえば、常に要求に基づいて、または指定されたユーザにのみアクセスを許可する場合、エンド ユーザ アクセスを設定できますが、スパム通知は設定できません。

エンド ユーザ隔離へのアクセスの設定

電子メール ユーザが、Cisco IronPort スパム隔離で自身のメッセージを管理できるようにします。

手順

ステップ 1　セキュリティ管理アプライアンスで、[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）] を選択します。

ステップ 2　[Cisco IronPort スパム隔離の設定（Cisco IronPort Spam Quarantine Settings）] セクションで [設定を編集（Edit Settings）] をクリックします。

ステップ 3　[エンドユーザの隔離へのアクセス（End-User Quarantine Access）] セクションまでスクロールします。

ステップ 4　[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ンにします。

ステップ 5　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 ユーザを認証する方式を指定します。メールボックス認証、LDAP 認証、または「なし」を指定できます。

- **メールボックス認証**：認証用の LDAP ディレクトリがないサイトの場合、スパム隔離では、ユーザのメールボックスを保有している標準の IMAP サーバまたは POP サーバにユーザの電子メール アドレスとパスワードを照合することができます。Web UI にログインするとき、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。隔離はこの情報を使用し、そのユーザとしてメールボックス サーバにログインします。ログインに成功すると、そのユーザは認証され、スパム隔離はユーザの受信箱を変更せずにメールボックス サーバからログアウトします。LDAP ディレクトリを使用しないサイトには、メールボックス認証が推奨されます。ただし、メールボックス認証では、複数の電子メール エイリアスに送信された隔離済みメッセージを表示できません。

  メールボックス サーバのタイプ（IMAP または POP）を選択します。サーバ名と、安全な接続に SSL を使用するかどうかを指定します。サーバのポート番号を入力します。未修飾のユーザ名の後ろに追加するドメイン（company.com など）を入力します。

POP サーバがバナーに APOP サポートをアドバタイズする場合は、セキュリティの理由から（すなわち、パスワードがクリアな状態で送信されないように）、アプライアンスでは APOP だけを使用します。一部のユーザで 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 サーバを再設定する必要があります。

- [LDAP] : LDAP サーバまたはアクティブなエンド ユーザ認証クエリーが設定されていない場合は、[Management Appliance] > [システム管理（System Administration）] > [LDAP] リンクを選択して、LDAP サーバ設定とエンド ユーザ認証クエリー ストリングを設定します。LDAP 認証の設定の詳細については、「LDAP サーバ プロファイルの作成」（P.11-2）を参照してください。
- [なし（None）] : 認証をイネーブルにしなくても、Cisco IronPort スパム隔離へのエンド ユーザのアクセスを許可できます。この場合、ユーザは通知メッセージのリンクをクリックして隔離にアクセスでき、システムはメールボックス認証または LDAP 認証を行いません。

ステップ 6　隔離から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が選択されていると、[Cisco IronPort スパム隔離（Cisco IronPort Spam Quarantine）] ページでメッセージ本文を表示できなくなります。代わりとして、隔離されたメッセージを表示するには、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 7　変更を送信し、保存します。

エンドユーザのためのスパム通知の設定

スパム通知とは、Cisco IronPort スパム隔離内にメッセージが捕捉されているときに、電子メール ユーザに送信される電子メール メッセージのことです。通知には、そのユーザ宛の隔離されたスパムまたはその疑いのあるメッセージのリストが含まれます。さらに、各ユーザがそれぞれの隔離されたメッセージを表示できるリンクも含まれます。イネーブルにすると、指定したスケジュールに従って通知が送信されます。

スパム通知を使用すると、エンド ユーザが LDAP 認証またはメールボックス認証を使用しないでスパム隔離にログインできるようになります。ユーザは、受信した電子メール通知を介して隔離にアクセスします（その隔離に対して通知がイネーブルになっている場合）。メッセージの件名をクリックすると、ユーザは隔離の Web UI にログインします。

（注）　このログイン方式では、そのエンド ユーザが持っている可能性のある他のエイリアス宛の隔離済みメッセージは表示されません。また、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。

アプライアンスがスパム通知を生成する方法でそのようになっているため、ユーザは、自分の電子メール エイリアス宛の複数のスパム通知を受信することがあります。また、複数の電子メール アドレスを使用しているユーザも、複数のスパム通知を受信することがあります。複数の通知は、エイリアス統合機能を使用して一部の発生を防ぐことができます。**LDAP サーバまたはアクティブなエイリアス統合クエリーが設定されていない場合は、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] を選択して、LDAP サーバ設定とエイリアス統合クエリー ストリングを設定します。**詳細については、「エンドユーザのためのスパム管理機能の設定」（P.7-9）を参照してください。

手順

ステップ 1　セキュリティ管理アプライアンスで、[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）] を選択します。

ステップ 2　[Cisco IronPort スパム隔離の設定（Cisco IronPort Spam Quarantine Settings）] セクションで [設定を編集（Edit Settings）] をクリックします。

ステップ 3　[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て、スパム通知をイネーブルにします。

ステップ 4　通知の [送信元アドレス（From Address）] を入力します。このアドレスを、ユーザの電子メール クライアントでサポートされている「ホワイトリスト」に追加することもできます。

ステップ 5　通知の [件名（Subject）] を入力します。

ステップ 6　カスタマイズする通知の [タイトル（Title）] を入力します。

ステップ 7　[デフォルト言語（Default Language）] を選択します。

ステップ 8　メッセージ本文をカスタマイズします。AsyncOS では、メッセージ本文に挿入されると、個々のエンド ユーザに対応した実際の値に展開されるいくつかのメッセージ変数がサポートされています。たとえば、**%username%** は、そのユーザへの通知が生成されるときに、実際のユーザ名に展開されます。サポートされるメッセージ変数には、次のものがあります。

- [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%**）：エンド ユーザ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%**）：スパム隔離にログインし、メッセージを表示するための URL。
- [Username]（**%username%**）
- [新規メッセージ一覧（New Message Table）]（**%new_quarantine_messages%**）：隔離領域内にあるこのユーザ宛の新しいメッセージのリスト

これらのメッセージ変数は、[メッセージ本文（Message Body）] フィールドのテキスト内に直接入力して、メッセージ本文に挿入できます。あるいは、変数を挿入する場所にカーソルを配置してから、右側の [メッセージ変数（Message Variables）] リスト内にある変数の名前をクリックすることもできます。

ステップ 9　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 10　バウンス アドレスを指定します。バウンスされた通知は、このアドレスに送信されます。

ステップ 11　必要に応じて、異なるアドレスで同じ LDAP ユーザに送信されたメッセージを統合できます。

ステップ 12　通知スケジュールを設定します。通知を月に一度、週に一度、または毎日（平日のみ、または週末も含めて）の指定した時間に送信するように設定できます。

ステップ 13　変更を送信し、保存します。

エンド ユーザのセーフリスト/ブロックリスト機能の設定と管理

エンド ユーザによるセーフリストとブロックリストの作成を許可して、スパムとして処理する電子メール メッセージをより適切に制御できます。セーフリストによって、指定されたユーザおよびドメインからのメールがスパムとして処理されないようにできます。ブロックリストでは、他のユーザおよびドメインからのメールが常にスパムとして処理されるようにします。セーフリスト/ブロックリスト機能がイネーブルにされると、各エンド ユーザは、自分の電子メール アカウントに対してセーフリストとブロックリストを維持できるようになります。

（注）　セーフリストやブロックリストを設定しても、メッセージに対するウイルスのスキャンや、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は、電子メール セキュリティ アプライアンスで実行されます。セーフリストのメンバーから送信されたメッセージの場合、他のスキャン設定に従って配信されない場合があります。

ユーザがセーフリストまたはブロックリストにエントリを追加すると、そのエントリは セキュリティ管理アプライアンス上のデータベースに保管され、関連するすべての 電子メール セキュリティ アプライアンスで、定期的に更新および同期されます。同期の詳細については、「セーフリストとブロックリストの設定とデータベースの同期」（P.7-13）を参照してください。データベースのバックアップの詳細については、「セーフリスト/ブロックリスト データベースのバックアップと復元」（P.7-15）を参照してください。

セーフリストとブロックリストは、エンド ユーザによって作成およびメンテナンスされます。ただし、この機能をイネーブルにし、ブロックリスト内のエントリに一致する電子メール メッセージの配信設定を設定するのは管理者です。セーフリストとブロックリストは Cisco IronPort スパム隔離に関連するため、配信の動作は、他のアンチスパム設定にも左右されます。電子メール パイプラインでメッセージが電子メール セキュリティ マネージャに到達する前に発生する処理に基づいて、メッセージがアンチスパム スキャンをスキップすることがあります。メッセージ処理に関する詳細情報については、お使いの電子メール セキュリティ アプライアンス のマニュアルまたはオンライン ヘルプの「Understanding the Email Pipeline」を参照してください。

たとえば、アンチスパム スキャンをスキップするように HAT で「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では、自分のセーフリストとブロックリストの設定をそのリスナー上で受信されたメールに適用しないようになります。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。

セーフリスト/ブロックリスト メッセージの配信の詳細については、「セーフリストとブロックリストのメッセージ配信」（P.7-14）を参照してください。

セキュリティ管理アプライアンスでのセーフリスト/ブロックリストのイネーブル化と設定

セーフリスト/ブロックリスト機能をイネーブル化する前に、アプライアンスで Cisco IronPort スパム隔離をイネーブル化する必要があります。Cisco IronPort スパム隔離のイネーブル化の詳細については、「中央集中型スパム隔離の設定」（P.7-2）を参照してください。

手順

ステップ 1　セキュリティ管理アプライアンスで、[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）] を選択します。

ステップ 2　[End-User Safelist/Blocklist] セクションで [有効（Enable）] をクリックします。

ステップ 3　[エンド ユーザ セーフリスト/ブロックリス（End-User Safelist/Blocklist）] セクションで [設定を編集（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）] チェックボックスがオンになっていることを確認します。

ステップ 5　ユーザごとの最大リスト項目数を指定します。この値は、ユーザがそれぞれのセーフリスト/ブロックリストに含めることのできるアドレスとドメインの最大数です。デフォルトは 100 です。

（注）　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　更新頻度を選択します。この値によって、AsyncOS がシステムにある 電子メール 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 データベースを更新する頻度が決まります。M10、M600、および M650 アプライアンスのデフォルトは、2 時間ごとです。M1000 および M1050 アプライアンスのデフォルトは、4 時間ごとです。

ステップ 7　変更を送信し、保存します。

ステップ 8　この機能の中央集中化をサポートするよう、電子メール セキュリティ アプライアンスを設定します。「電子メール セキュリティ アプライアンスでのセーフリスト/ブロックリストの設定」（P.7-13）を参照してください。

電子メール セキュリティ アプライアンスでのセーフリスト/ブロックリストの設定

管理対象の電子メール セキュリティ アプライアンスでセーフリスト/ブロックリストの設定を行うには、**それぞれの**電子メール セキュリティ アプライアンスで次の手順を実行してください。

手順

ステップ 1　電子メール セキュリティ アプライアンスで、[セキュリティ サービス（Security Services）] > [外部スパム隔離（External Spam Quarantine）] を選択します。

ステップ 2　[設定を編集（Edit Settings）] ボタンをクリックします。

ステップ 3　セーフリスト/ブロックリスト機能をイネーブルにするチェックボックスを選択します。

ステップ 4　ブロックリストに含まれる送信者からのメッセージを隔離するか、削除するかを選択します。

ステップ 5　変更を送信し、保存します。

ステップ 6　管理対象の電子メール セキュリティ アプライアンスに対して、この手順を繰り返します。

セーフリストとブロックリストの設定とデータベースの同期

セキュリティ管理アプライアンスを使用すると、簡単に、すべての管理対象アプライアンスでセーフリスト/ブロックリスト データベースを同期することができます。

（注）　セーフリスト/ブロックリスト データベースを同期する前に、セーフリスト/ブロックリスト機能をイネーブル化して、少なくとも 1 台の管理対象アプライアンスを セキュリティ管理アプライアンスに追加する必要があります。管理対象アプライアンスを追加する方法の詳細については、「管理対象アプライアンスの追加について」（P.2-12）を参照してください。

セーフリスト/ブロックリスト データベースを同期するには、[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）] ページで [すべてのアプライアンスを同期（Synchronize All Appliances）] ボタンをクリックします。

集中管理機能を使用して複数のアプライアンスを設定する場合は、集中管理を使用して管理者設定を設定できます。集中管理を使用しない場合は、マシン間で設定が整合していることを手動で確認できます。

FTP を使用してアプライアンスにアクセスする方法の詳細については、付録 A「IP インターフェイスおよびアプライアンスへのアクセス」（P.1）を参照してください。

セーフリストとブロックリストのメッセージ配信

セーフリストとブロックリストをイネーブルにすると、電子メール セキュリティ 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。アプライアンスがエンド ユーザのセーフリスト/ブロックリスト設定に一致する送信者またはドメインを検出したとき、セーフリスト/ブロックリスト設定が異なる受信者が複数存在すると、そのメッセージは分割されます。たとえば、送信者 X が受信者 A と受信者 B の両方にメッセージを送信したとします。受信者 A のセーフリストには送信者 X のエントリがありますが、受信者 B のセーフリストにもブロックリストにも、この送信者の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 に送信されたメッセージには、*X-SLBL-Result-Safelist* ヘッダーによって、セーフリストに登録されているというマークが付けられます。これにより、アンチスパム スキャンがスキップされます。受信者 B に宛てられたメッセージは、アンチスパム スキャン エンジンでスキャンされます。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、配信の動作は、ブロックリスト アクション設定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ップされます。

（注）　ブロックリスト アクションは、電子メール セキュリティ アプライアンスの外部スパム隔離設定で指定します。詳細については、「中央集中型スパム隔離のための電子メール セキュリティ アプライアンスの設定」（P.7-6）を参照してください。

メッセージを隔離するようにブロックリスト アクションを設定した場合、メッセージはスキャンされ、最終的に隔離されます。メッセージを削除するようにブロックリスト アクションを設定した場合、セーフリスト/ブロックリスト スキャンの直後にメッセージは削除されます。

セーフリスト/ブロックリスト データベースのバックアップと復元

セーフリスト/ブロックリスト データベースのバックアップを維持できるように、セキュリティ管理アプライアンスでデータベースを .csv ファイルとして保存できます。.csv ファイルは、アプライアンスの設定が格納される XML コンフィギュレーション ファイルとは別に保管されます。アプライアンスをアップグレードする場合、またはシステム セットアップ ウィザードを実行する場合、まず、セーフリスト/ブロックリスト データベースを .csv ファイルにバックアップする必要があります。

（注） .csv ファイルを編集してからアップロードすると、個別のエンド ユーザのセーフリストおよびブロックリストを変更できます。

データベースをバックアップすると、アプライアンスによって、.csv ファイルが次の命名規則に従って `/configuration` ディレクトリに保存されます。

slbl-<serial number>-<timestamp>.csv

セキュリティ管理アプライアンスをバックアップするときには、セーフリストおよびブロックリストのデータベースを対象に含めるかどうかを選択できます 「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」（P.14-7）を参照してください。

手順

ステップ 1　セキュリティ管理アプライアンスで、[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 2　[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。

ステップ 3　データベースを .csv ファイルにバックアップするには、[今すぐバックアップ（Backup Now）] をクリックします。

ステップ 4　[リストアするファイルを選択（Select File to Restore）] をクリックして、データベースを復元します。

アプライアンスにより、`/configuration` ディレクトリに保管されているバックアップ ファイルのリストが表示されます。

ステップ 5　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、[リストア（Restore）] をクリックします。

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

エンド ユーザは、自分のセーフリストとブロックリストを管理します。管理者が、エンド ユーザ アカウントにそのユーザのログイン名とパスワードでログインすると、エンド ユーザのセーフリストまたはブロックリストにアクセスできます。または、管理者はセーフリスト/ブロックリスト データベースのバックアップ バージョンをダウンロードして、個別のユーザのリストを編集できます。

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 メッセージがセーフリスト/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_logs またはアンチスパム ログ ファイルにロギングされます。

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」（P.14-33）を参照してください。

ログ ファイルの詳細については、第 15 章「ロギング」を参照してください。

エンド ユーザのセーフリストおよびブロックリストの使用

エンド ユーザは、指定した送信者からのメッセージをスパムの判定から除外するために、セーフリストを作成できます。また、指定した送信者からのメッセージを常にスパムとして扱うために、ブロックリストを使用できます。たとえば、エンド ユーザは、受信したくない電子メールをメーリング リストから受信する場合があります。この送信者をブロックリストに追加すると、この送信者からの電子メール メッセージが配信されないようになります。一方、エンド ユーザは、正当な送信者からの電子メール メッセージが Cisco IronPort スパム隔離に送信されていることに気づき、この電子メール メッセージがスパムとして処理されないようにしたいと考えることがあります。その送信者からのメールが隔離されないようにするには、ユーザのセーフリストに送信者を追加します。

（注）　セーフリスト/ブロックリスト設定は、システム管理者が設定する他の設定の影響を受けます。たとえば、セーフリストに登録されているメッセージが、ウイルス陽性と判断された場合、または管理者によって内容が企業の電子メール ポリシーに準拠していないと判断された場合、このメッセージは配信されません。

セーフリストとブロックリストへのアクセス

LDAP 認証またはメールボックス（IMAP または POP）認証を使用してアカウントが認証されるエンド ユーザは、セーフリストとブロックリストにアクセスするために、Cisco IronPort スパム隔離の自分のアカウントにログインする必要があります。これらのエンド ユーザは、通常はスパム通知経由でメッセージにアクセスしているとしても（この場合は一般に LDAP 認証またはメールボックス認証を必要としません）、自分のアカウントにログインしなければなりません。エンド ユーザ認証が [なし（None）] に設定されている場合、エンド ユーザは、セーフリスト/ブロックリスト設定にアクセスする際に自分のアカウントにログインする必要はありません。

セーフリストおよびブロックリストへのエントリの追加

エントリ（IPv6 アドレスを使用するものを含む）をセーフリスト/ブロックリストに追加するときには、次の形式を使用できます。

- user@domain.com

  user@[203.0.113.15]

  user@[ipv6:2001:db8:80:1::5]
- server.domain.com
- domain.com

  [203.0.113.15]

  [ipv6:2001:db8:80:1::5]

エンド ユーザは、同じ送信者またはドメインをセーフリストとブロックリストの両方に同時には追加できません。ただし、ある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ユーザをブロックリストに追加した場合、両方のルールが適用されます（逆の場合も同様です）。たとえば、エンド

ユーザが *example.com* をセーフリストに追加し、*george@example.com* をブロックリストに追加すると、アプライアンスは、example.com からのすべてのメールをスパムかどうかスキャンせずに配信しますが、*george@example.com* からのメールはスパムとして処理します。

エンド ユーザは、.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、ブロックしたりはできません。ただし、エンド ユーザは、server.domain.com のような構文を使用して、特定のドメインを明示的にブロックすることはできます。

セーフリストの操作

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。Cisco IronPort スパム隔離から、グラフィカル ユーザ インターフェイスの右上にある [オプション（Options）] メニューをクリックし、[セーフリスト（Safelist）] を選択して、手動で送信者をセーフリストに追加できます。

電子メール アドレスまたはドメインをリストに追加し、[リストに追加（Add to List）] をクリックします。

エンド ユーザは、メッセージが Cisco IronPort スパム隔離に送信されていても、その送信者をセーフリストに追加できます。特定の送信者からのメッセージが Cisco IronPort スパム隔離に捕捉されている場合、エンド ユーザはそのメッセージの横にあるチェックボックスをオンにして、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）] を選択できます。

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。

（注） エンド ユーザは、スパム通知メッセージを使用してメッセージを解放することもできます。[スパムではない（Not Spam）] リンクをクリックして、特定のメッセージを解放します。送信者をエンド ユーザのセーフリストに追加するオプションもあります。

ブロックリストの操作

エンド ユーザは、ブロックリストを使用して、指定した送信者からのメールが配信されないようにできます。送信者をブロックリストに追加するには、エンド ユーザ隔離から [オプション（Options）] > [ブロックリスト（Blocklist）] を選択します。

エンド ユーザ隔離から、フィールドに電子メール アドレスまたはドメインを入力し、[リストに追加（Add to List）] をクリックします。

電子メール セキュリティ アプライアンスは、ブロックリスト内のエントリと一致する電子メール アドレスまたはドメインからのメールを受信すると、そのメールをスパムとして処理します。ブロックリスト アクション設定に応じて、そのメールは削除または隔離されます。

Cisco IronPort スパム隔離内のメッセージの管理

ここでは、管理者が Cisco IronPort スパム隔離内のメッセージを管理する方法について説明します。管理者が隔離を表示する場合、その隔離領域に含まれるすべてのメッセージを利用できます。

（注）　メッセージを表示および管理するグラフィカル ユーザ インターフェイスは、Cisco IronPort スパム隔離にアクセスするエンド ユーザ用のものとは少し異なります。エンド ユーザ用のグラフィカル ユーザ インターフェイスについては、エンド ユーザとして Cisco IronPort スパム隔離にアクセスし、オンライン ヘルプを参照してください。

管理者として、Cisco IronPort スパム隔離内のメッセージに対して次のアクションを実行できます。

- メッセージの表示
- メッセージの配信
- メッセージの削除
- メッセージの検索

Cisco IronPort スパム隔離内でのメッセージの検索

手順

ステップ 1　セキュリティ管理アプライアンスで、[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [スパム隔離（Spam Quarantine）] を選択します。

ステップ 2　[スパム隔離（Spam Quarantine）] リンクを選択します。

ステップ 3　検索フォームで、検索する日付を入力します。現在の日、または過去の週からメッセージを検索できます。または、カレンダー アイコンをクリックして、日付範囲を選択できます。

ステップ 4　オプションで、差出人アドレス、受取人アドレス、メッセージ件名のテキスト文字列を指定します。入力した値が検索結果に含まれる、含まれない、全体と一致、先頭と一致、末尾と一致のいずれかを選択します。

ステップ 5　オプションで、エンベロープ受信者を指定します。入力した値が検索結果に含まれる、含まれない、全体と一致、先頭と一致、末尾と一致のいずれかを選択します。

エンベロープ受信者とは、「RCPT TO」SMTP コマンドで定義されている電子メール メッセージ受信者のアドレスです。エンベロープ受信者は、「Recipient To」アドレスまたは「Envelope To」アドレスと呼ばれることもあります。

ステップ 6　[検索（Search）] をクリックします。

検索条件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。

大量メッセージの検索

Cisco IronPort スパム隔離内に大量のメッセージが保存されており、検索条件が狭く定義されていない場合、検索結果の表示に時間がかかることや、クエリーがタイムアウトすることがあります。

その場合、検索を再実行するかどうか確認されます。

（注）　大量の検索を同時に複数実行すると、アプライアンスのパフォーマンスに悪影響を与えることがあります。

Cisco IronPort 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、Cisco IronPort スパム隔離内のメッセージが表示されます。1 ページに表示されるメッセージの数を選択できます。カラム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。再度カラム見出しをクリックすると、ソートの順を反転できます。

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。[メッセージの詳細（Message Details）] ページには、メッセージの先頭 20K が表示されます。メッセージがそれよりも長い場合は、20K に切り詰められます。ページの下部にあるリンクをクリックすると、メッセージの残りの部分が表示されます。

[メッセージの詳細（Message Details）] ページから、[削除（Delete）] を選択してメッセージを削除したり、[リリース（Release）] を選択してメッセージを隔離から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。

HTML メッセージの表示

Cisco IronPort 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。イメージは表示されません。

符号化されたメッセージの表示

Base64 で符号化されたメッセージは、復号化されてから表示されます。

Cisco IronPort スパム隔離内のメッセージの配信

メッセージを配信のために解放するには、メッセージの隣にあるチェックボックスを選択して、[リリース（Release）] をクリックします。

ページに表示されているすべてのメッセージを選択するには、見出し行にあるチェックボックスをオンにします。

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。

Cisco IronPort スパム隔離からのメッセージの削除

Cisco IronPort スパム隔離では、指定された時間後にメッセージが自動で削除されるように設定できます。Cisco IronPort 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横にあるチェックボックスをオンにして、[削除（Delete）] をクリックします。ページに表示されているすべてのメッセージを選択するには、見出し行にあるチェックボックスをオンにします。

Cisco IronPort スパム隔離内のすべてのメッセージを削除するには、[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）] ページから隔離をディセーブルにして、表示される [すべて削除（Delete All）] をクリックします。