

CHAPTER 7

Cisco IronPort スпам検疫の管理

この章は、次の項で構成されています。

- 「Cisco IronPort スпам検疫について」 (P.7-1)
- 「IronPort スпам検疫の設定」 (P.7-3)
- 「エンド ユーザ アクセスと通知の設定」 (P.7-7)
- 「スパムを転送する電子メールセキュリティ アプライアンスの設定」 (P.7-12)
- 「Cisco IronPort スпам検疫内のメッセージの管理」 (P.7-15)
- 「エンド ユーザのセーフリスト/ブロックリスト機能のイネーブル化」 (P.7-19)
- 「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」 (P.7-24)

Cisco IronPort スпам検疫について

Cisco IronPort スпам検疫は、エンド ユーザ宛のスパムおよびその疑いのあるメッセージを保管するために使用される、特別な種類の検疫です。(エンド ユーザとはメール ユーザのことで、AsyncOS ユーザではありません)。ローカルな Cisco IronPort スпам検疫は、電子メールセキュリティ アプライアンスに常駐しています。メッセージを、別の Cisco IronPort アプライアンス (通常は Security Management アプライアンス) に常駐している外部の Cisco IronPort スпам検疫に送信することもできます。



(注) システム検疫は Email Security アプライアンスに常駐し、コンテンツ フィルタリング、スキャンング、感染フィルタの適用など、AsyncOS が実行するさまざまなアクションに基づいて検疫されたメッセージを保持します。

Cisco IronPort スпам検疫は「誤検出」（正規の電子メールがスパムとして検疫または削除されること）が問題になる組織にセーフガード メカニズムを提供します。Cisco IronPort スпам検疫を使用すると、メッセージをスパムであると最終的に判断する前に、エンド ユーザおよび管理者が、スパムのフラグが設定されたメッセージを確認できます。さらに、セーフリスト/ブロックリスト機能がイネーブルの場合、エンド ユーザはスパムのマークが付けられたメッセージに対して制御を実行できます。



(注) 指定されたユーザまたはユーザ グループに対してのみ、Cisco IronPort スпам検疫へのエンド ユーザ アクセスを実装できます。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 ユーザが検疫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。

スパムおよびその疑いのあるメッセージが検疫されたことをユーザに通知する電子メールを送信するように、AsyncOS を設定することができます。通知には、現在 Cisco IronPort スпам検疫エリアにあるそのユーザ宛のメッセージのサマリーが含まれます。ユーザはメッセージを表示し、電子メール受信トレイに送信するか、削除するかを決定できます。また、ユーザは検疫されたメッセージを検索できます。通知メッセージを通じて検疫にアクセスすることも、Web ブラウザを使用して直接検疫にアクセスすることもできます。（検疫にエンド 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 ユーザ検疫へのアクセスの設定](#)」(P.7-8) を参照してください)。

デフォルトでは、Cisco IronPort スпам検疫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検疫スペースがすべて消費されることを避けるために、AsyncOS は Cisco IronPort スпам検疫から定期的にメールを削除します。

すべての Administrator レベルのユーザ（デフォルトの admin ユーザなど）は、Cisco IronPort スпам検疫へのアクセスおよび変更ができます。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検疫へのアクセス権が割り当てられているユーザは、検疫の内容の表示および管理ができますが、検疫設定の変更はできません。Cisco IronPort スпам検疫へのエンド 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、検疫エリアにある自分のメッセージにアクセスできます。

IronPort スпам検疫の設定


Cisco IronPort スпам検疫設定を Security Management アプライアンスで編集する前に、Cisco IronPort スпам検疫サービスを Security Management アプライアンスでイネーブルにする必要があります。サービスをイネーブルにする方法の詳細については、「[Security Management アプライアンスでの Cisco IronPort スпам検疫のイネーブル化とディセーブル化](#)」(P.3-8) を参照してください。

Cisco IronPort スпам検疫設定を編集するには、次の手順を実行します。

-
- ステップ 1** Security Management アプライアンスのウィンドウで、[Management Appliance] > [Centralized Services] > [Spam Quarantine] を選択します。
- ステップ 2** [Cisco IronPort Spam Quarantine Settings] セクションで [Edit Settings] をクリックします。
- [Edit Cisco IronPort Spam Quarantine] ページが表示されます。

図 7-1 Cisco IronPort スпам検疫設定の編集

Edit IronPort Spam Quarantine

Spam Quarantine Settings	
<input checked="" type="checkbox"/> Enable IronPort Spam Quarantine	
Quarantine IP Interface:	Management ▾
Quarantine Port:	11
Deliver Messages Via:	<p>Notifications and released messages will be delivered by the server(s) specified below.</p> <p>Primary Server: 127.0.0.1 Port: 25 IronPort Appliance or SMTP Server IP Address</p> <p>Alternative Server: 127.0.0.1 Port: 25</p> <p><i>Note: You must configure your destination server(s) to accept mail from this host. If you are delivering to an IronPort Appliance, it must be configured to direct spam to this appliance. See the IronPort documentation for more information.</i></p>
Schedule Delete After:	<input checked="" type="radio"/> 14 days <input type="radio"/> Do not schedule delete
Default Language:	English/United States [en-us] ▾
Notify IronPort Upon Message Release:	<input type="checkbox"/> Send a copy of released messages to IronPort for analysis(recommended)
Spam Quarantine Appearance:	<p>Current Logo:  IRONPORT Spam Quarantine</p> <p><input checked="" type="radio"/> Use Current Logo</p> <p><input type="radio"/> Use IronPort Spam Quarantine Logo</p> <p><input type="radio"/> Upload Custom Logo: <input type="text"/> Browse... Maximum size 500w x 50h pixels</p> <p>Login Page Message: <input type="text"/></p>
Administrative Users	
<p>You have no 'operator' users defined in your system. Go to System Administration > to configure users. Members of the "Administrator" group have full access to Quarantines and will automatically be granted access to the IronPort Spam Quarantine.</p>	

- ステップ 3** [Quarantine IP Interface] セクションで、検疫に使用する適切な IP インターフェイスとポートを、ドロップダウン リストから指定します。
- デフォルトでは、検疫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 Security Management アプライアンスのインターフェイスです。検疫ポートは、送信アプライアンスが外部検疫設定で使用しているポート番号です。
- ステップ 4** [Deliver Messages Via] セクションで、メールを配信するプライマリ宛先および代替宛先を、対応するテキスト フィールドに入力します。
- 宛先は、SMTP、グループウェア サーバ、または別のアプライアンスです。
- ステップ 5** [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、[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、検疫を設定することを推奨します。検疫エリアの容量がいっぱいになると、古いメッセージから順に削除されます。

ステップ 6 [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пам検疫にアクセスしたときに表示される言語です。

ステップ 7 (任意) 解放されたメッセージのコピーを分析のために Cisco IronPort に送信するには、[Notify Cisco IronPort upon Message Release] で、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、検疫を設定することを推奨します。

ステップ 8 (任意) [Spam Quarantine Appearance] セクションで、エンド ユーザが検疫を表示した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。

- Use Current logo
- Use Cisco IronPort Spam Quarantine logo
- Upload Custom logo

[Upload Custom logo] を選択した場合、ユーザがログインして検疫されたメッセージを表示すると、Cisco IronPort スпам検疫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пам検疫のロゴが使用されます。

ステップ 9 (任意) [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 ユーザに対して検疫へのログイン プロンプトを表示するときに表示されます。

ステップ 10 オプションで、Cisco IronPort スпам検疫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пам検疫の管理ユーザの設定](#)」(P.7-6) を参照してください。

ステップ 11 オプションで、エンド ユーザ 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 アクセスと通知の設定](#)」(P.7-7) を参照してください。

ステップ 12 変更を送信し、保存します。

Cisco IronPort スпам検疫の管理ユーザの設定

Cisco IronPort スпам検疫のメッセージを管理する役割を、他のユーザに分散できます。他のユーザがこの機能にアクセスできるようにするには、このセクションの手順を使用してください。

Operator、Read-Only Operator、Help Desk、Guest のいずれかのロールが割り当てられているか、スパム検疫へのアクセス権が含まれているカスタム ユーザロールが割り当てられたユーザが、スパム検疫のメッセージを管理できます。

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、常にスパム検疫にアクセスできるので、この手順を使用してスパム検疫機能に関連付ける必要はありません。



(注) Administrator レベルでないユーザは、スパム検疫エリアのメッセージにアクセスできますが、検疫設定の編集はできません。Administrator レベルのユーザは、メッセージへのアクセスと設定の編集ができます。

ユーザがスパム検疫を管理できるようにするには、次の手順を実行します。

- ステップ 1** ユーザを作成し、そのユーザにスパム検疫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.12-43) を参照してください。
- ステップ 2** Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Spam Quarantine] を選択します。
- ステップ 3** [Spam Quarantine Settings] セクションで、[Enable] または [Edit Settings] をクリックします。[Edit Spam Quarantine] ページが表示されます。
- ステップ 4** [Spam Quarantine Settings] セクションの [Administrative Users] 領域で、[Local Users]、[Externally Authenticated Users]、または [Custom User Roles] の選択リンクをクリックします。
- ステップ 5** スпам検疫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 [Administrative Users] にリストされているその他のタイプ ([Local Users]、[Externally Authenticated Users]、または [Custom User Roles]) について繰り返します。

ステップ 8 [Submit] をクリックし、変更内容を確定させます。

エンド ユーザ アクセスと通知の設定

基本的な Cisco IronPort スпам検疫設定の他に、検疫のその他の設定ができます。追加の設定は、[Edit Cisco IronPort Spam Quarantine] ページの [Spam Quarantine Settings] セクションの下に表示されます。

次の追加設定ができます。

- [End user access to the quarantine] : 詳細については、「[エンド ユーザ検疫へのアクセスの設定](#)」(P.7-8) を参照してください。
- [Spam notifications] : 詳細については、「[スパム通知のイネーブル化](#)」(P.7-9) を参照してください。

追加の設定にアクセスするには、[Management Appliance] > [Centralized Services] > [Spam Quarantine] を選択して、[Cisco IronPort Spam Quarantine Settings] セクションの [Edit Settings] ボタンをクリックします。[Edit Cisco IronPort Spam Quarantine] ページをスクロールダウンして、追加の設定を表示します。

図 7-2 Cisco IronPort スпам検疫の追加設定の編集

End-User Quarantine Access	
<input type="checkbox"/>	Enable End-User Quarantine Access
<i>Enabling this feature allow end-users to access and manage their suspected spam quarantine. Users with access will be able to view, search, release and delete messages from their quarantine.</i>	
Spam Notifications	
<input type="checkbox"/>	Enable Spam Notification
<i>Enabling Spam Notification causes email notifications to be sent in digest format, listing a summary of all messages quarantined since the last notification. See example.</i>	
<input type="button" value="Cancel"/>	<input type="button" value="Submit"/>



(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 ユーザ検疫へのアクセスの設定

Cisco IronPort スпам検疫へのエンド ユーザ アクセスを設定するには、次の手順を実行します。

- ステップ 1** Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Spam Quarantine] を選択します。
- ステップ 2** [Cisco IronPort Spam Quarantine Settings] セクションで [Edit Settings] をクリックします。[Edit Cisco IronPort Spam Quarantine] ページが表示されます。
- ステップ 3** [Edit Cisco IronPort Spam Quarantine] ページの [Enable End-User Quarantine Access] チェックボックスをオンにします。

図 7-3 Cisco IronPort スпам検疫へのエンド ユーザアクセスのイネーブル化

- ステップ 4** エンド ユーザが検疫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、または認証なしを使用できます。
 - [Mailbox authentication] : 認証用の LDAP がないサイトの場合、検疫は、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できます。Web UI にログインしたときに、ユーザは電子メール アドレスとパスワードを入力します。検疫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、検疫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検疫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）、アプライアンスは APOP のみを使用します。一部のユーザに対して 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。

- [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] > [System Administration] > [LDAP] 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tring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.10-3) を参照してください。
- [None] : 認証をイネーブルにしなくても、Cisco IronPort スпам検疫へのエンド 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検疫にアクセスでき、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 5 検疫からメッセージを解放する前に、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、Cisco IronPort スпам検疫ページからメッセージ本文を表示できなくなります。代わりとして、検疫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 6 [Submit] をクリックし、[Commit] をクリックして変更を確定します。

スパム通知のイネーブル化

スパム通知とは、Cisco IronPort スпам検疫内にメッセージが存在するときに、エンド 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、そのユーザ宛の検疫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検疫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、[Edit Cisco IronPort Spam Quarantine] ページで指定され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 またはメールボックス認証を使用せずに検疫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検疫にアクセスします（その検疫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、ユーザは検疫の 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検疫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検疫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、[Management Appliance] > [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tring を設定します。詳細については、「[エンド ユーザ アクセスと通知の設定](#)」(P.7-7) を参照してください。

スパム通知を設定するには、次の手順を実行します。

-
- ステップ 1** Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Spam Quarantine] を選択します。
- ステップ 2** [Cisco IronPort Spam Quarantine Settings] セクションで [Edit Settings] をクリックします。
- [Edit Cisco IronPort Spam Quarantine] ページが表示されます。
- ステップ 3** [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。

図 7-4 スпам通知の設定

Spam Notifications	
<input checked="" type="checkbox"/> Enable Spam Notification	
From Address:	"friendly name" (optional) <username@hostname> (example: "Email Administrator" <notify@company.com>)
Subject:	IronPort Spam Quarantine Notification
Title:	IronPort Spam Quarantine Notification
Message Body:	<p>The message(s) below have been blocked by your administrator as suspected spam.</p> <p>There are %new_message_count% new messages in your Email Quarantine since you received your last IronPort Quarantine Notification. If the messages below are spam, you do not need to take any action. Messages will be automatically removed from the quarantine after %days_until_expire% day(s).</p> <p>If any of the messages below are not spam, click the Release link to have them sent to your Inbox. To see all quarantined messages view %quarantine_url%. Preview Message</p>
Message Format:	HTML (recommended)
Deliver Bounce Message To:	(e.g. mybounceaddress@company.com)
Consolidate Notifications:	<input type="checkbox"/> Consolidate notifications sent to the same LDAP user at different addresses <i>This setting uses the LDAP Alias Consolidation Query configured at System Administration > LDAP.</i>
Notification Schedule:	<input type="radio"/> Monthly (Sent the 1st of each month at 12am) <input checked="" type="radio"/> Weekly Monday (Sent at 12am) <input type="radio"/> Daily (weekdays)
	<input type="checkbox"/> 12 <input type="checkbox"/> 3 <input type="checkbox"/> 6 <input type="checkbox"/> 9 AM <input type="checkbox"/> 12 <input type="checkbox"/> 3 <input type="checkbox"/> 6 <input type="checkbox"/> 9 PM

- ステップ 4** 通知の差出人アドレスを入力します。ユーザは、このアドレスを、自分の電子メールクライアントでサポートされる「ホワイトリスト」に追加できます。
- ステップ 5** 通知の件名を入力します。
- ステップ 6** 通知のカスタマイズされたタイトルを入力します。
- ステップ 7** 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。

- [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
- [Total Message Count] (%total_message_count%) : エンド ユーザ検疫内にあるこのユーザ宛のメッセージの数
- [Days Until Message Expires] (%days_until_expire%)

- [Quarantine URL] (%quarantine_url%) : 検疫にログインし、メッセージを表示するための URL
- [Username] (%username%)
- [New Message Table] (%new_quarantine_messages%) : 検疫エリア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、[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 [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 8** 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 9** 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 10** 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 11** 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 12** [Submit] をクリックし、[Commit] をクリックして変更を確定します。

スパムを転送する電子メール セキュリティ アプリアランスの設定

Security Management アプリアランスで Cisco IronPort スпам検疫を設定した後、Email Security アプリアランスが Security Management アプリアランスにスパムまたはその疑いのあるメッセージを転送するようにシステムで設定する必要があります。

スパムを転送するように Email Security アプリアランスを設定するには、次のタスクを実行します。

- **外部検疫の設定** : Email Security アプリアランスの外部検疫設定で、Security Management アプリアランス名および Cisco IronPort スпам検疫用の接続情報を指定する必要があります。詳細については、「[外部検疫の設定](#) (P.7-13) を参照してください。

- **管理対象アプライアンスの追加または更新** : Email Security アプライアンスを Security Management アプライアンスの管理対象アプライアンスとして追加または更新する必要があります。また、Email Security アプライアンスからのスパムを検疫するオプションを選択する必要があります。詳細については、「[管理対象アプライアンスの追加と更新、および検疫スパム オプションの使用](#)」(P.7-14) を参照してください。

外部検疫の設定

Email Security アプライアンスで Security Management アプライアンスの Cisco IronPort スпам検疫を使用するには、Email Security アプライアンスの外部検疫を設定する必要があります。



(注)

これまで、Email Security アプライアンスに別の外部スパム検疫を設定していた場合は、まず、その外部スパム検疫設定をディセーブルにする必要があります。

外部検疫を設定するには、次の手順を**すべての** Email Security アプライアンスで実行する必要があります。

- ステップ 1** [Security Services] > [External Spam Quarantine] ページで、[Configure] ボタンをクリックします。
- ステップ 2** チェックボックスを選択して、外部スパム検疫をイネーブルにします。
- ステップ 3** Cisco IronPort スпам検疫の名前を入力します。検疫がある Security Management 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 4** Security Management アプライアンスの管理インターフェイスの IP アドレスを入力します。
- ステップ 5** スпам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。ここで入力するポート番号は、Security Management アプライアンスのグラフィカル ユーザ インターフェイスの [Edit Cisco IronPort Spam Quarantine] ページで入力した検疫ポート番号と同じにする必要があります。詳細については、「[IronPort スпам検疫の設定](#)」(P.7-3) を参照してください。
- ステップ 6** オプションで、チェックボックスを選択し、セーフリスト/ブロックリスト機能をイネーブルにします。セーフリスト/ブロックリスト機能をイネーブルにする場合は、ブロックリストに含まれている送信者からのメッセージを検疫するか、

削除するかを選択します。セーフリスト/ブロックリスト機能の詳細については、「[エンドユーザのセーフリスト/ブロックリスト機能のイネーブル化](#)」(P.7-19) を参照してください。

ステップ 7 [Submit] をクリックし、[Commit] をクリックして変更を確定します。

管理対象アプライアンスの追加と更新、および検疫スパム オプションの使用

Email Security アプライアンスで Security Management アプライアンスの Cisco IronPort スпам検疫を使用するには、Security Management アプライアンスの管理対象アプライアンスとして追加する必要があります。または、すでに Email Security アプライアンスが管理対象アプライアンスとして追加されている場合は、検疫スパム オプションを使用するように管理対象アプライアンス設定を更新する必要があります。

Security Management アプライアンスで [Management Appliance] > [Centralized Services] > [Security Appliances] を選択し、管理対象 Email Security アプライアンスを追加します。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](#)」(P.3-11) を参照してください。



注意

管理対象アプライアンスを追加するときに、アプライアンスからのスパムを検疫するようにオプションを選択してください。

すでに Email Security アプライアンスが Security Management アプライアンスの管理対象アプライアンスとして存在する場合は、検疫スパム オプションを使用するように管理対象アプライアンス設定を更新する必要があります。

検疫スパム オプションを使用するように管理対象アプライアンス設定を更新するには、次の手順を実行します。

ステップ 1 Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Security Appliances] を選択します。

ステップ 2 セキュリティ アプライアンスのリストで、Email Security アプライアンスの名前をクリックします。

ステップ 3 [Edit Appliance: <appliance_name>] ページで、[図 7-5](#) に示すように、アプライアンスからのスパムを検疫するオプションを選択します。

図 7-5 スпамを検疫するための管理対象アプライアンスの編集

Edit Appliance: example.srv

Security Appliance	
Appliance Name:	example.srv
IP Address:	111.11.1.11
Centralized Services:	<input checked="" type="checkbox"/> Quarantine spam from this appliance <input type="checkbox"/> Centralized reporting: all available host licenses in use <input type="checkbox"/> Centralized tracking: all available host licenses in use
File Transfer Access:	Not configured. <small>File transfer access via ssh is required for transfer of reporting data, message tracking data, and quarantine Safelist/Blocklist data</small>
<input type="button" value="Test Configuration"/> <input type="button" value="Configure File Transfer Access..."/>	
<input type="button" value="Cancel"/> <input type="button" value="Submit"/>	

ステップ 4 [Submit] をクリックし、[Commit] をクリックして変更を確定します。

Cisco IronPort スпам検疫内のメッセージの管理

ここでは、管理者が Cisco IronPort スпам検疫内のメッセージを管理する方法について説明します。管理者が検疫を表示する場合、その検疫エリア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пам検疫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пам検疫にアクセスし、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пам検疫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пам検疫内のメッセージにアクセスするには、次の手順を実行します。

- ステップ 1** Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Spam Quarantine] を選択します。
- ステップ 2** [Cisco IronPort Spam Quarantine] リンクをクリックします。
[Spam Quarantine Search] ページが表示されます。

図 7-6 [Spam Quarantine Search] ページ

Spam Quarantine Search

- ステップ 3** [Submit] をクリックし、[Commit] をクリックして変更を確定します。

Cisco IronPort スпам検疫内でのメッセージの検索

Cisco IronPort スпам検疫内のメッセージを検索するには、次の手順を実行します。

- ステップ 1** Security Management アプライアンスで、[Email] > [Message Quarantine] > [Spam Quarantine] を選択します。
- ステップ 2** 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 3 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 4 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 5 [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 [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пам検疫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пам検疫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пам検疫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。[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。

[Message Details] ページから、[Delete] を選択してメッセージを削除したり、[Release] を選択してメッセージを検疫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пам検疫では、HTML ベースのメッセージは近似で表示されません。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пам検疫内のメッセージの配信

メッセージを解放して配信するには、メッセージの横のチェックボックスをオンにして [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пам検疫からのメッセージの削除

Cisco IronPort スпам検疫では、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пам検疫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、[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пам検疫内のすべてのメッセージを削除するには、検疫をディセーブルにして（「[Security Management アプライアンスでの Cisco IronPort スпам検疫のイネーブル化とディセーブル化](#)」（P.3-8）を参照）、[Management Appliance] > [Centralized Services] > [Spam Quarantine] ページの [Delete All] リンクをクリックします。

エンドユーザのセーフリスト/ブロックリスト機能のイネーブル化

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なります。ブロックリストによって、その他のユーザおよびドメインからのメールは常にスパムとして処理されます。セーフリストとブロックリストの設定は、Cisco IronPort スпам検疫から設定されます。そのため、Cisco IronPort スпам検疫をイネーブルにし、この機能を使用するように設定する必要があります。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、Email Security 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 Security Management 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 Email Security 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.7-22）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.7-21) 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пам検疫に関連するため、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。メッセージ処理の詳細については、『*Cisco IronPort AsyncOS for Email User Guide*』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。

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.7-23) を参照してください。

セーフリスト/ブロックリスト設定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пам検疫をイネーブル化する必要があります。Cisco IronPort スпам検疫のイネーブル化の詳細については、「[Security Management アプライアンスでの Cisco IronPort スпам検疫のイネーブル化とディセーブル化](#)」(P.3-8) を参照してください。

Security Management アプライアンスでセーフリスト/ブロックリスト機能をイネーブル化および設定するには、次の手順を実行します。

-
- ステップ 1** Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Spam Quarantine] を選択します。
 - ステップ 2** [End-User Safelist/Blocklist] セクションで [Enable] をクリックします。
 - ステップ 3** [End-User Safelist/Blocklist] セクションで [Edit Settings] をクリックします。
 - ステップ 4** [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、ユーザが各セーフリストおよびブロックリストに含めることのできるアドレスまたは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** 更新の頻度を選択します。この値によって、AsyncOS がシステムにある Email Security 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** [Submit] をクリックし、[Commit] をクリックして変更を確定します。

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、Security Management 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

GUI から、次の方法を使用して、データベースのバックアップおよび復元を実行できます。

- ステップ 1** Security Management アプライアンスで、[Management Appliance] > [System Administration] > [Configuration File] を選択します。
- ステップ 2** [End-User Safelist/Blocklist Database] セクションに移動します。

- 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、[Backup Now] をクリックします。
- ステップ 4** データベースを復元するには、[Select File to Restore] をクリックします。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、[Restore] をクリックします。

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

Security Management 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 Security Management 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](#)」(P.3-11) 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、[Management Appliance] > [Centralized Services] > [Spam Quarantine] ページで [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 「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、Email Security 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 データベースに対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場合、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裂します。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 に送信されるメッセージは、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検疫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、Email Security アプライアンスの外部スパム検疫設定で指定します。詳細については、「[外部検疫の設定](#)」(P.7-13) を参照してください。

メッセージを検疫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、最終的に検疫されます。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。管理者は、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.12-82) を参照してください。

ログファイルの詳細については、第 13 章「ロギング」(P.1) 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。ユーザは、この送信者をユーザのブロックリストに追加して、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することができます。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пам検疫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検疫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пам検疫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 [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

各エントリは、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

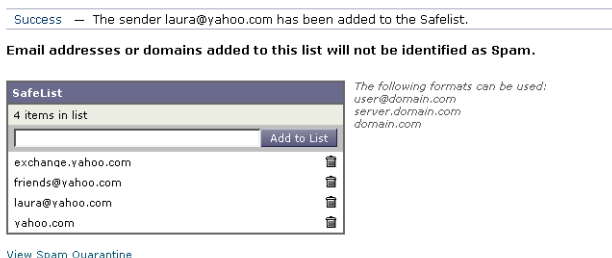
エンド ユーザは、同じ送信者またはドメインをセーフリストとブロックリストの両方に同時には追加できません。ただし、あるドメインをセーフリストに追加し、そのドメインに所属するユーザをブロックリストに追加した場合、両方のルールが適用されます (逆の場合も同様です)。たとえば、エンド ユーザが *example.com* をセーフリストに追加し、*george@example.com* をブロックリストに追加すると、アプライアンスは、*example.com* からのすべてのメールをスパムかどうかスキャンせずに配信しますが、*george@example.com* からのメールはスパムとして処理します。

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пам検疫から、グラフィカル ユーザ インターフェイスの右上にある [Options] メニューをクリックし、[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。

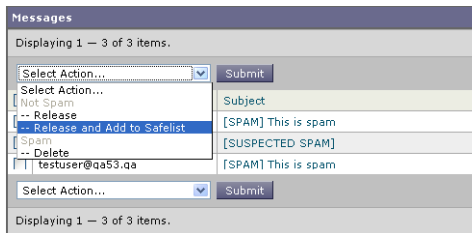
図 7-7 エンドユーザ検疫のセーフリスト



電子メール アドレスまたはドメインをリストに追加し、[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пам検疫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пам検疫に保持されている場合、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 [Release and Add to Safelist] を選択できます。

図 7-8 エンドユーザ検疫のセーフリスト



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。



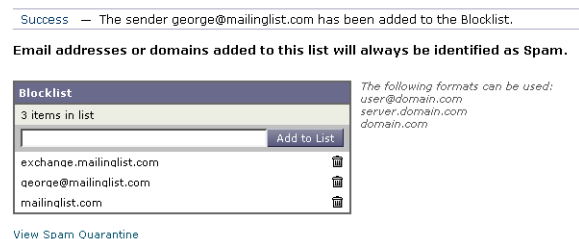
(注)

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。[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、エンドユーザ検疫から [Options] > [Blocklist] を選択します。

図 7-9 ブロックリストへの送信者の追加



エンドユーザ検疫から、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、[Add to List] をクリックします。

Email Security 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検疫されます。