CHAPTER 8

集約ポリシー、ウイルス、およびアウトブレイク隔離

- 「集約隔離の概要」（P.8-1）
- 「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）
- 「ポリシー、ウイルス、およびアウトブレイク隔離の管理」（P.8-9）
- 「ポリシー、ウイルス、アウトブレイク隔離内のメッセージの操作方法」（P.8-17）

集約隔離の概要

電子メール セキュリティ アプライアンス上の特定のフィルタ、ポリシー、およびスキャン操作により処理されたメッセージは、次の作業に備えて一時的に保管するために隔離内に置くことができます。シスコのコンテンツ セキュリティ管理アプライアンスの複数の電子メール セキュリティ アプライアンスからの隔離を集約できます。

集約隔離には次のような利点があります。

- 複数の電子メール セキュリティ アプライアンスから隔離されたメッセージを 1 箇所で管理できます。
- 隔離されたメッセージは、DMZ 内ではなくファイアウォールの背後に保存され、セキュリティ リスクを減らします。
- セキュリティ管理アプライアンスの標準のバック アップ機能の一部として、集約隔離はバックアップできます。

次の 2 種類の隔離を集約できます。

- ポリシー、ウイルス、アウトブレイク隔離

  ウイルス対策スキャンおよびアウトブレイク フィルタのどちらにも専用の隔離があります。メッセージ フィルタリング、コンテンツ フィルタリング、およびデータ漏洩防止ポリシーで検出されたメッセージを保持するためのポリシー隔離を作成します。

- スパム隔離

  第 7 章「Cisco IronPort スパム隔離の管理」を参照してください。

追加情報については、電子メール セキュリティ アプライアンスのマニュアルの「Quarantines」の章を参照してください。

隔離の種類

隔離領域タイプ	隔離名	デフォルトではシステムで作成されるか	説明	詳細情報
ウイルス	ウイルス	Yes	ウイルス対策エンジンによって判定されたため、マルウェアを送信する可能性のあるメッセージを保留します。	• 「ポリシー、ウイルス、およびアウトブレイク隔離の管理」（P.8-9） • 「ポリシー、ウイルス、アウトブレイク隔離内のメッセージの操作方法」（P.8-17）
アウトブレイク	アウトブレイク	Yes	スパムまたはマルウェアの可能性があるためアウトブレイク フィルタによって検出されたメッセージを保留します。	
ポリシー	ポリシー	Yes	メッセージ フィルタ、コンテンツ フィルタ、および DLP メッセージ アクションによって検出されたメッセージを保留します。 デフォルトのポリシー隔離が作成されています。	
	未分類	Yes	メッセージ フィルタ、コンテンツ フィルタ、または DLP メッセージ アクションで指定された隔離が削除されている場合のみメッセージを保留します。 この隔離はどのフィルタまたはメッセージ アクションにも割り当てることはできません。	
	（自分で作成したポリシー隔離）	No	メッセージ フィルタ、コンテンツ フィルタ、および DLP メッセージ アクションで使用するために作成するポリシー隔離。	
スパム	スパム	Yes	メッセージの受信者または管理者がレビューするためにスパム メッセージまたはサスペクト スパム メッセージを保留します。	第 7 章「Cisco IronPort スパム隔離の管理」

ポリシー、ウイルス、およびアウトブレイク隔離の集約

	手順	詳細情報
ステップ 1	ご使用の電子メール セキュリティ アプライアンスが DMZ 内にあり、セキュリティ管理アプライアンスがファイアウォールの背後にある場合は、アプライアンスが集約ポリシー、ウイルス、およびアウトブレイク隔離データを交換できるようにファイアウォール内のポートを開きます。	付録 C「ファイアウォール情報」
ステップ 2	セキュリティ管理アプライアンスで、この機能を有効にします。	「セキュリティ管理アプライアンスでの集約ポリシー、ウイルス、およびアウトブレイク隔離のイネーブル化」（P.8-4）
ステップ 3	セキュリティ管理アプライアンスで、非スパム隔離用ディスク領域を割り当てます。	「ディスク使用量の管理」（P.14-56）
ステップ 4	（オプション） • 必要な設定でセキュリティ管理アプライアンスに集約ポリシー隔離を作成します。 • 集約ウイルスおよびアウトブレイク隔離を設定します。 移行の前にこれらの設定を設定する場合、ご使用の電子メール セキュリティ アプライアンスの既存設定を参照できます。 カスタム移行の設定中に必要な隔離を作成することも、または自動移行の際に隔離が作成されるようにすることもできます。移行中に作成されたすべての隔離はデフォルト設定です。 ローカルの隔離の設定は隔離名が同じでも集約隔離では保持されません。	「ポリシー隔離の作成」（P.8-12）
ステップ 5	セキュリティ管理アプライアンスで、管理する電子メール セキュリティ アプライアンスを追加するか、追加済みアプライアンスの集約管理サービスから [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus and Outbreak Quarantines）] オプションを選択します。 ご使用の電子メール セキュリティ アプライアンスがクラスタ化されている場合、特定のレベル（マシン、グループ、またはクラスタ）に属するすべてのアプライアンスは、そのクラスタ内の任意の電子メール セキュリティ アプライアンスで集約された [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus and Outbreak Quarantines）] を有効にする前に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。	「管理対象の各電子メールセキュリティ アプライアンスへの集約ポリシー、ウイルス、アウトブレイク隔離サービスの追加」（P.8-5）
ステップ 6	変更を保存します。	—
ステップ 7	セキュリティ管理アプライアンスで、電子メール セキュリティ アプライアンスから既存のポリシー隔離の移行を設定します。	「ポリシー、ウイルス、アウトブレイク隔離の移行の設定」（P.8-6）

	手順	詳細情報
ステップ 8	電子メール セキュリティ アプライアンスで、集約ポリシー、ウイルス、およびアウトブレイク隔離機能を有効にします。 **重要**： 電子メール セキュリティ アプライアンスでポリシー、ウイルス、およびアウトブレイク隔離を設定済みの場合、隔離およびすべてのメッセージの移行はこの変更を確定するとすぐに開始します。	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の「Centralizing Services on a Cisco Content セキュリティ管理アプライアンス」の章の、特に次の項を参照してください。 • 「About Migration of Policy, Virus, and Outbreak Quarantines」 • 「Centralizing Policy, Virus, and Outbreak Quarantines」
ステップ 9	追加の電子メール セキュリティ アプライアンスを移行します。 一度に 1 つの移行プロセスだけしか処理できない可能性があります。前の移行が完了する前に、別の電子メール セキュリティ アプライアンスの集約ポリシー、ウイルス、およびアウトブレイク隔離を有効にしないでください。	—
ステップ 10	必要に応じて集約隔離設定を編集します。 移行中に作成された隔離は、集約および内部隔離名が同じでも元の内部隔離での設定ではなくデフォルト設定で作成されます。	「ポリシー隔離の作成」（P.8-12）
ステップ 11	メッセージ フィルタ、コンテンツ フィルタ、および DLP メッセージ アクションが集約隔離の名前で自動的に更新できない場合、お使いの電子メール セキュリティ アプライアンスのこれらの設定を手動で更新します。 クラスタ設定では、フィルタおよびメッセージ アクションがそのレベルで定義されている場合に限り、フィルタおよびメッセージ アクションは特定のレベルで自動的に更新できます。	お使いの電子メール セキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドのメッセージ フィルタ、コンテンツ フィルタ、および DLP メッセージ アクションのついてのマニュアルを参照してください。
ステップ 12	（推奨）元のアプライアンスが使用できない場合、リリースされたメッセージを処理するために電子メール セキュリティ アプライアンスを指定します。	「リリースされたメッセージを処理する代替アプライアンスの指定」（P.8-8）
ステップ 13	カスタム ユーザ ロールに管理を委任する場合、特定の方法でアクセスを設定する必要があります。	「カスタム ユーザ ロールの集約隔離アクセスの設定」（P.8-8）

セキュリティ管理アプライアンスでの集約ポリシー、ウイルス、およびアウトブレイク隔離のイネーブル化

はじめる前に

「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）の表に記載されたこの手順の前までの手順をすべて完了してください。

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）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 2　[有効（Enable）] をクリックします。

ステップ 3　電子メール セキュリティ アプライアンスと通信するためインターフェイスとポートを次のように指定します。

- これらを変更する理由がない限り、デフォルトの選択を受け入れます。
- 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。
- ファイアウォールで開いたポートと同じポートを使用します。

ステップ 4　[送信（Submit）] をクリックします。

次の作業

「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）内の表の次のステップに戻ります。

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集約ポリシー、ウイルス、アウトブレイク隔離サービスの追加

すべての電子メール セキュリティ アプライアンスのすべての隔離の統合ビューを表示するには、すべての隔離を集約する前にすべての電子メール セキュリティ アプライアンスを追加することを検討してください。

はじめる前に

「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）の表に記載されたここまでのすべての手順を完了したことを確認します。

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）] > [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.　[ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] 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（Appliance Name）] および[IP アドレス（IP Address）] テキスト フィールドに、追加している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 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.　[ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] サービスはあらかじめ選択されています。

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。

ステップ 4　[送信（Submit）] をクリックします。

ステップ 5　[ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を有効にする各電子メール 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て行ってください。

たとえば、クラスタ内の他のアプライアンスを追加します。

ステップ 6　変更を保存します。

次の作業

「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）内の表の次のステップに戻ります。

ポリシー、ウイルス、アウトブレイク隔離の移行の設定

はじめる前に

- 「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）の表に記載されたここまでのすべての手順を完了したことを確認します。
- 移行プロセスに関する警告や情報については、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の「Centralizing Services on a Cisco Content セキュリティ管理アプライアンス」の章の「About Migration of Policy, Virus, and Outbreak Quarantines」の項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）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 2　[移行ウィザードの起動（Launch Migration Wizard）] をクリックします。

ステップ 3　移行方法を選択します。

条件	選択	その他の情報
• すべての関連する電子メール セキュリティ アプライアンスからのすべての既存ポリシー隔離を移行する場合、 および • 同じ名前のポリシー隔離をすべての電子メール セキュリティ アプライアンス上で同一の設定にする場合、 および • すべての電子メール セキュリティ アプライアンス上で同じ名前を持つすべてのポリシー隔離をこの名前を持つ単一の集約ポリシー隔離にマージする場合	自動（Automatic）	このプロセスを使用して作成されたすべての集約ポリシー隔離は、電子メール セキュリティ アプライアンスの同じ名前の隔離の設定に関係なく、デフォルト設定で自動的に設定されます。 移行後にこれらの設定を更新する必要があります。
• 同じ名前のポリシー隔離が別の電子メール セキュリティ アプライアンス上で異なる設定になっていてこの違いを維持する場合、 または • 内部隔離の一部を移行し、他のすべてを削除する場合、 または • 内部隔離を異なった名前の集約隔離に移行する場合 または • 単一の集約隔離に異なる名前の内部隔離をマージする場合	カスタム（Custom）	移行前ではなく移行中に作成するすべての集約ポリシー隔離は新しい隔離に対するデフォルト設定で設定されます。 移行後にこれらの設定を更新する必要があります。

ステップ 4　[次へ（Next）] をクリックします。

ステップ 5　[自動（Automatic）] を選択した場合、次の手順に従います。

移行するポリシー隔離および必要なこのページの他の情報を確認します。

ウイルスおよびアウトブレイク隔離も移行されます。

ステップ 6　[カスタム（Custom）] を選択した場合、次の手順に従います。

- すべての電子メール セキュリティ アプライアンスからの隔離を表示するか、または 1 つだけからの隔離を表示するかを選択するには、[隔離の表示元（Show Quarantines from）] リストから選択肢を選択します。
- 各集約ポリシー隔離に移動する内部ポリシー隔離を選択します。
- 必要に応じて追加の集約ポリシー隔離を作成します。これらはデフォルト設定になります。
- 隔離名は大文字と小文字が区別されます。
- 左のテーブルに残っている隔離は移行されず、移行時に電子メール セキュリティ アプライアンスから削除されます。
- 右のテーブルから隔離を選択し [集約隔離から削除（Remove from Centralized Quarantine）] をクリックして隔離のマッピングを変更できます。

ステップ 7　必要に応じて [次へ（Next）] をクリックします。

ステップ 8　変更を送信し、保存します。

次の作業

「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）内の表の次のステップに戻ります。

リリースされたメッセージを処理する代替アプライアンスの指定

通常、メッセージが集約隔離からリリースされるとき、セキュリティ管理アプライアンスは最初にそのメッセージを集約隔離に送信した電子メール セキュリティ アプライアンスで処理するためにこれを返します。

メッセージの発信元の電子メール セキュリティ アプライアンスが利用可能でない場合、リリースされたメッセージを別の電子メール セキュリティ アプライアンスで処理し配信できます。この目的のアプライアンスを指定します。

はじめる前に

- リリースされたメッセージを代替アプライアンスで処理して配信できそうか確認します。たとえば、暗号化とアンチウイルス再スキャンの設定は、プライマリ アプライアンスの同じ設定と一致する必要があります。
- 代替アプライアンスは、集約ポリシー、ウイルス、およびアウトブレイク隔離に完全に設定する必要があります。そのアプライアンスに関して「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）の表の手順を実行します。

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）] > [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　[代替リリース アプライアンスの指定（Specify Alternate Release Appliance）] ボタンをクリックします。

ステップ 3　電子メール セキュリティ アプライアンスを選択します。

ステップ 4　変更を送信し、保存します。

関連項目

- 「電子メール セキュリティ アプライアンスが使用できないときのメッセージのリリース」（P.8-9）

カスタム ユーザ ロールの集約隔離アクセスの設定

カスタム ユーザ ロールを持つ管理者が電子メール セキュリティ アプライアンス上のメッセージおよびコンテンツ フィルタ内および DLP メッセージ アクション内で集約ポリシー隔離を指定できるようにするためには、セキュリティ管理アプライアンスの関連ポリシー隔離へのこれらのユーザ アクセスを許可し、セキュリティ管理アプライアンスに作成するカスタム ユーザ ロール名が電子メール セキュリティ アプライアンス上のものと一致する必要があります。

関連項目

- 「Custom Email User ロールの作成」（P.13-7）

集約ポリシー、ウイルス、およびアウトブレイク隔離のディセーブル化

通常、これらの集約隔離を無効にする必要がある場合は電子メール セキュリティ アプライアンスでそれを行う必要があります。

それを行った場合の影響のリストなど、集約ポリシー、ウイルス、アウトブレイク隔離の無効化の詳細については、お使いの電子メール セキュリティ アプライアンスのオンライン ヘルプまたはマニュアルを参照してください。

電子メール セキュリティ アプライアンスが使用できないときのメッセージのリリース

通常、メッセージが集約隔離からリリースされるとき、セキュリティ管理アプライアンスは最初にそのメッセージを集約隔離に送信した電子メール セキュリティ アプライアンスで処理するためにこれを返します。

メッセージの発信元の電子メール セキュリティ アプライアンスが利用可能でない場合、リリースされたメッセージを別の電子メール セキュリティ アプライアンスで処理し配信できます。この目的で、代替リリース アプライアンスを指定する必要があります。

代替アプライアンスが使用できない場合、代替リリース アプライアンスとして別の電子メール セキュリティ アプライアンスを指定できそのアプライアンスがキューに入っているメッセージを処理して配信します。

電子メール セキュリティ アプライアンスへの到達に繰り返し失敗した後に、アラートを受け取ります。

関連項目

- 「リリースされたメッセージを処理する代替アプライアンスの指定」（P.8-8）

ポリシー、ウイルス、およびアウトブレイク隔離の管理

- 「ポリシー、ウイルス、およびアウトブレイク隔離に対するディスク領域の割り当て」（P.8-10）
- 「隔離内のメッセージの保留時間」（P.8-10）
- 「自動的に処理される隔離メッセージのデフォルト アクション」（P.8-11）
- 「システム作成隔離の設定の確認」（P.8-11）
- 「ポリシー隔離の作成」（P.8-12）
- 「ポリシー、ウイルス、アウトブレイク隔離の設定の編集」（P.8-13）
- 「隔離を割り当てるフィルタおよびメッセージ アクションの決定」（P.8-13）
- 「ポリシー隔離の削除について」（P.8-14）
- 「隔離状態、容量、およびアクティビティのモニタリング」（P.8-14）
- 「隔離用のディスク容量の使用率に関するアラート」（P.8-15）
- 「ポリシー隔離とロギング」（P.8-15）

- 「メッセージ処理タスクの他のユーザへの配信について」（P.8-16）

ポリシー、ウイルス、およびアウトブレイク隔離に対するディスク領域の割り当て

ディスク領域の割り当てについては、「ディスク使用量の管理」（P.14-56）を参照してください。

複数の隔離内のメッセージは、単一の隔離内のメッセージと同じ容量のディスク領域を消費します。

アウトブレイク フィルタと集約隔離の両方が有効な場合、以下のようになります。

- 内部ポリシー、ウイルス、アウトブレイク隔離に割り当てられた電子メール セキュリティ アプライアンスのすべてのディスク領域が、アウトブレイク ルールが更新されるたびにこれらのメッセージをスキャンするために、アウトブレイク隔離内のメッセージのコピーを保留するために代わって使用されます。
- セキュリティ管理アプライアンス上のディスク領域は、電子メール セキュリティ アプライアンスの使用可能なディスク領域の容量によって制限される可能性があります。
- この状況の詳細については、「隔離内のメッセージの保留時間」（P.8-10）を参照してください。

関連項目

- 「隔離状態、容量、およびアクティビティのモニタリング」（P.8-14）
- 「隔離用のディスク容量の使用率に関するアラート」（P.8-15）
- 「隔離内のメッセージの保留時間」（P.8-10）

隔離内のメッセージの保留時間

メッセージは次の状況で隔離から自動的に削除されます。

- 通常の有効期限切れ：保留時間は、隔離内のメッセージに一致します。隔離ごとにメッセージの保留時間を指定します。各メッセージには、それぞれ独自の有効期限があり、リストに表示されます。このトピックで説明する別の状況が発生しなければ、メッセージは指定された時間だけ保留されます。

  （注）　アウトブレイク フィルタ内のメッセージの通常の保留時間は、アウトブレイク隔離内ではなく、電子メール ポリシーの [アウトブレイク フィルタ（Outbreak Filters）] セクションで設定されます。

- 早期の有効期限切れ：メッセージは設定されている保留時間に到達する前に隔離から強制的に削除されます。これは次の場合に発生する可能性があります。
  - 「ポリシー、ウイルス、およびアウトブレイク隔離に対するディスク領域の割り当て」（P.8-10）に定義されているすべての隔離のサイズ制限に達した。

    サイズ制限に達すると、隔離に関係なく、最も古いメッセージが処理されメッセージごとのデフォルト アクションが、すべての隔離のサイズが再度サイズ制限未満になるまで実行されます。このポリシーは、First In First Out（FIFO; 先入れ先出し）です。最新の有効期限に基づいて複数の隔離内のメッセージが期限切れになります。

（任意）ディスク領域が十分でないために個々の隔離がリリースまたは削除から除外されるように設定することができます。すべての隔離が除外されディスク領域が容量に達するように設定すると、セキュリティ管理アプライアンスで領域が利用可能になるまで、メッセージが電子メール セキュリティ アプライアンスに保留されます。

セキュリティ管理アプライアンスはメッセージをスキャンしないため、集約アウトブレイク隔離内の各メッセージのコピーは、最初にメッセージを処理した電子メール セキュリティ アプライアンスに保存されます。これによって電子メール セキュリティ アプライアンスはアウトブレイク フィルタ ルールが更新されるたびに隔離されているメッセージを再スキャンし、もう脅威とは見なされないメッセージをセキュリティ管理アプライアンスに伝えることができます。アウトブレイク隔離の両方のコピーは同時にメッセージの同じセットを保持する必要があります。したがって、電子メール セキュリティ アプライアンスのディスク領域に空きがなくなるというまれな状況では、両方のアプライアンスのアウトブレイク隔離内のメッセージのコピーは集約隔離にまだ領域がある場合でも、早く期限切れとなります。

ディスク領域のマイルストーンについてアラートを受け取ります。「隔離用のディスク容量の使用率に関するアラート」（P.8-15）を参照してください。

- まだメッセージを保留している隔離を削除する。

メッセージが隔離から自動的に削除される場合、そのメッセージでのデフォルト アクションが実行されます。「自動的に処理される隔離メッセージのデフォルト アクション」（P.8-11）を参照してください。

保留時間の時間調整の影響

- 夏時間とアプライアンスの時間帯の変更は保留時間に影響しません。
- 隔離の保留時間を変更すると、新しいメッセージだけが新しい有効期限を持ちます。
- システム クロックを変更すると、過去に終了しているはずのメッセージが次の最も適切な時間に期限切れになります。
- システム クロックの変更は期限切れになる処理中のメッセージには適用されません。

自動的に処理される隔離メッセージのデフォルト アクション

「隔離内のメッセージの保留時間」（P.8-10）で説明された状況のどれかが発生するとポリシー、ウイルス、アウトブレイク隔離内のメッセージでデフォルト アクションが実行されます。

以下の 2 つのプライマリ デフォルト アクションがあります。

- 削除：メッセージが削除されます。
- リリース：メッセージは配信するためにリリースされます。

  リリースの際に、メッセージはウイルス対策またはスパム対策エンジンによって再スキャンされる場合があります。詳細については、「隔離されたメッセージの再スキャンについて」（P.8-23）を参照してください。

  さらに、予定の保留時間が過ぎる前にリリースされたメッセージは、X ヘッダーの追加など、その他の操作を行うことができます。詳細については、「ポリシー隔離の作成」（P.8-12）を参照してください。

  集約隔離からリリースされたメッセージは、処理のために発生元の電子メール セキュリティ アプライアンスに返されます。

システム作成隔離の設定の確認

隔離を使用する前に、分類されていない隔離も含めデフォルト隔離の設定をカスタマイズします。

ポリシー隔離の作成

はじめる前に

- 保留時間およびデフォルト アクションを含め、隔離内のメッセージが自動的に管理される方法を理解します。「隔離内のメッセージの保留時間」（P.8-10）および「自動的に処理される隔離メッセージのデフォルト アクション」（P.8-11）を参照してください。
- 各隔離にアクセスするユーザを決定し、ユーザおよびカスタム ユーザ ロールを適宜作成します。詳細は、「隔離にアクセスできるユーザ グループ」（P.8-16）を参照してください。

手順

ステップ 1　[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 2　[ポリシー隔離を追加（Add Policy Quarantine）] をクリックします

ステップ 3　情報を入力します。

次の点を考慮してください。

- 隔離の名前は変更できません。
- 指定した保留期間の終了前にこの隔離内のメッセージを処理しないようにする場合は、隔離ディスク領域に空き領域がなくても、[容量オーバーフロー時にメッセージにデフォルトのアクションを適用して容量を解放します（Free up space by applying default action on messages upon space overflow）] を無効にします。

  すべての隔離でこのオプションを選択しないでください。少なくとも 1 つの隔離からメッセージを削除して、空き領域を作る必要があります。
- デフォルト アクションとして [リリース（Release）] を選択すると、保留期間が経過する前にリリースされるメッセージに適用される追加アクションを指定できます。

オプション	情報
件名の変更（Modify Subject）	テキストを入力し、元のメッセージの件名の先頭または末尾にそれを追加するかどうかを指定します。 たとえば、メッセージが不適切なコンテンツを含むかもしれないことを受信者に警告する場合があります。 **（注）**　非 ASCII 文字を含む件名を正しく表示するために、件名は RFC 2047 に従って表記されている必要があります。

オプション	情報
X-Header を追加（Add X-Header）	[X-Header を追加（Add X-Header）] では、メッセージの措置の記録を提供できます。これは、たとえば特定のメッセージが配信された理由に関する照会に対処するときなどに役に立ちます。 名前と値を入力します。 例： 名前 =「`Inappropriate-release-early` 」 値 =「`True` 」
添付ファイルを除去（Strip Attachments）	添付ファイルを除去することで、このようなファイルに内包する可能性のあるウイルスから保護します。

ステップ 4　この隔離にアクセスできる次のユーザを指定します。

ユーザ	情報
ローカルユーザ（Local Users）	ローカル ユーザ リストには隔離にアクセスできるロールを持つユーザだけが含まれます。 すべての管理者は隔離に自由にアクセスできるため、このリストでは管理権限を持つユーザを除外します。
外部認証されたユーザ（Externally Authenticated Users）	外部認証を設定する必要があります。
カスタム ユーザ ロール（Custom User Roles）	隔離へのアクセス権を持つカスタム ユーザ ロールを少なくとも 1 つ作成した場合にのみ、このオプションが表示されます。

ステップ 5　変更を送信し、保存します。

次の作業

- まだ電子メール セキュリティ アプライアンスから隔離を移行していない場合、次の手順に従います。

  移行処理の一部としてこれらの隔離をメッセージ フィルタやコンテンツ フィルタおよび DLP メッセージ アクションに割り当てます。

- すでに集約隔離に移行した場合は、次の手順に従います。

  お使いの電子メール セキュリティ アプライアンスに隔離にメッセージを移動するメッセージ フィルタやコンテンツ フィルタおよび DLP メッセージ アクションがあることを確認します。電子メール セキュリティ アプライアンスのユーザ ガイドまたはオンライン ヘルプを参照してください。

ポリシー、ウイルス、アウトブレイク隔離の設定の編集

（注）
- 隔離の名前は変更できません。

- 「保留時間の時間調整の影響」（P.8-11）も参照してください。

隔離の設定を変更するには、[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、隔離の名前をクリックします。

隔離を割り当てるフィルタおよびメッセージ アクションの決定

隔離に関連付けられたメッセージ フィルタ、コンテンツ フィルタ、DLP メッセージ アクション、およびそれぞれが設定されている電子メール セキュリティ アプライアンスを表示できます。

手順

ステップ 1　[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] をクリックします。

ステップ 2　検査するポリシー隔離の名前をクリックします。

ステップ 3　ページの下部にスクロールして [関連付けられたメッセージ フィルタ / コンテンツ フィルタ /DLP メッセージ アクション（Associated Message Filters/Content Filters/DLP Message Actions）] を表示します。

ポリシー隔離の削除について

- ポリシー隔離を削除する前に、実行中のフィルタまたはメッセージ アクションと関連付けられているかどうかを確認します。「隔離を割り当てるフィルタおよびメッセージ アクションの決定」（P.8-13）を参照してください。
- フィルタまたはメッセージ アクションに割り当てられている場合でも、ポリシー隔離を削除できます。
- 空でない隔離を削除する場合、ディスクに空き領域がない場合にメッセージを削除しないというオプションを選択しても、隔離で定義されたデフォルト アクションがすべてのメッセージに適用されます。「自動的に処理される隔離メッセージのデフォルト アクション」（P.8-11）を参照してください。
- フィルタまたはメッセージ アクションと関連付けられた隔離を削除した後、このフィルタまたはメッセージ アクションにより引き続き隔離されたメッセージはすべて未分類隔離に送信されます。隔離を削除する前に、未分類隔離のデフォルト設定をカスタマイズする必要があります。
- 未分類隔離は削除できません。

隔離状態、容量、およびアクティビティのモニタリング

内容	手順
すべての非スパム隔離に割り当てられている領域の合計	[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、ページの最初のセクションで確認します。 割り当てを変更するには、「ディスク使用量の管理」（P.14-56）を参照してください。
すべての非スパム隔離で現在使用できる領域	[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、テーブルのすぐ下で確認します。
すべての隔離で現在使用中の合計容量	[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [システム ステータス（System Status）] を選択します。
各隔離で現在使用中の容量	[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、隔離名をクリックして、テーブルの隔離名のすぐ下にある行でこの情報を確認します
すべての隔離内の現在のメッセージの総数	[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [システム ステータス（System Status）] を選択します。
各隔離内にある現在のメッセージ数	[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、テーブルのその隔離の行を確認します。
すべての隔離による総 CPU 使用率	[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [システム ステータス（System Status）] を選択して [システム情報（System Information）] セクションで確認します。
最後のメッセージが各隔離に送信された日時（隔離間の移動を除く）	[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、テーブルのその隔離の行を確認します。
ポリシー隔離が作成された日付 ポリシー隔離の作成者の名前	[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、隔離名をクリックして、テーブルの隔離名のすぐ下にある行でこの情報を確認します 作成日および作成者の名前はシステムが作成した隔離では使用されません。
隔離に関連付けられたフィルタおよびメッセージ アクション	「隔離を割り当てるフィルタおよびメッセージ アクションの決定」（P.8-13）を参照してください。

隔離用のディスク容量の使用率に関するアラート

ポリシー、ウイルス、アウトブレイク隔離の合計サイズが容量の 75 パーセント、85 パーセント、95 パーセントに達するか超えると常にアラートが送信されます。このチェックは、メッセージが隔離エリアに入れられたときに実行されます。たとえば、隔離へのメッセージの追加でサイズが増加し総容量の 75 % になるかまたは超えると、アラートが送信されます。

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。

ポリシー隔離とロギング

AsyncOS により、隔離されるすべてのメッセージが個別にロギングされます。

```
Info: MID 482 quarantined to "Policy" (message filter:policy_violation)
```

括弧内には、メッセージを隔離させたメッセージ フィルタまたは Outbreak フィルタ機能のルールが出力されます。メッセージが入れられる隔離ごとに独立したログ エントリが生成されます。

また、AsyncOS により、隔離エリアから除去されるメッセージも個別にロギングされます。

```
Info: MID 483 released from quarantine "Policy" (queue full)
```

```
Info: MID 484 deleted from quarantine "Anti-Virus" (expired)
```

メッセージがすべての隔離から除去され、完全に削除されるか、配信用にスケジュールされると、それらのメッセージはシステムによって次のように個別にロギングされます。

```
Info: MID 483 released from all quarantines
```

```
Info: MID 484 deleted from all quarantines
```

メッセージが再注入されると、新しいメッセージ ID（MID）を持つ新しいメッセージ オブジェクトが作成されます。このことは、次のように「署名入り」の新しい MID を伴う既存のログ メッセージを使用してロギングされます。

```
Info: MID 483 rewritten to 513 by Policy Quarantine
```

メッセージ処理タスクの他のユーザへの配信について

メッセージのレビューおよび処理のタスクを他の管理者ユーザへ配信できます。次に例を示します。

- 人事部門はポリシー隔離をレビューし管理できます。
- 法務部門は社外秘マテリアル隔離を管理できます。

隔離の設定を指定するときに、これらのユーザにアクセス権限を割り当てます。隔離にユーザを追加するには、追加するユーザがすでに存在している必要があります。

各ユーザは、すべてまたは一部の隔離にアクセスできるようにすることも、まったくアクセスできないようにすることもできます。隔離の閲覧を許可されていないユーザに対しては、GUI または CLI の隔離のリスト表示のどこにも、その隔離の存在を示す証拠は一切表示されません。

関連項目

- 「隔離にアクセスできるユーザ グループ」（P.8-16）
- 第 13 章「管理タスクの分散」

隔離にアクセスできるユーザ グループ

ユーザが隔離にアクセスできるようにするときは、実行できるアクションは、次のユーザ グループごとに異なります。

- 管理者または電子メール管理者グループのユーザは、隔離の作成、設定、削除、および集約ができ、隔離メッセージを管理できます。
- オペレータ、ゲスト、読み込み専用オペレータ、およびヘルプ デスクのユーザ グループは、隔離管理権限を持つカスタム ユーザ ロール同様、隔離内のメッセージの検索、表示、および処理ができますが、隔離の設定を変更したり、隔離を作成、削除、または集約することはできません。それぞれの隔離にこれらのどのユーザがその隔離にアクセスするのかを指定します。
- Technicians グループに属するユーザは隔離にアクセスできません。

メッセージ トラッキングおよびデータ漏洩防止などの関連機能のアクセス権限も、[隔離（Quarantine）] ページに表示されるオプションおよび情報に影響します。たとえば、ユーザにメッセージ トラッキングへのアクセス権限がない場合、そのユーザは隔離されたメッセージに関するメッセージ トラッキング情報を確認できません。

（注） セキュリティ管理アプライアンスに設定されたカスタム ユーザ ロールがフィルタおよび DLP メッセージ アクションのポリシー隔離を指定できるようにするには、「カスタム ユーザ ロールの集約隔離アクセスの設定」（P.8-8）を参照してください。

ポリシー、ウイルス、アウトブレイク隔離内のメッセージの操作方法

- 「隔離内のメッセージの表示」（P.8-17）
- 「ポリシー、ウイルス、アウトブレイク隔離内メッセージの検索」（P.8-18）
- 「手動での隔離内のメッセージの処理」（P.8-19）
- 「複数の隔離内のメッセージ」（P.8-20）
- 「メッセージの詳細およびメッセージ コンテンツの表示」（P.8-21）
- 「隔離されたメッセージの再スキャンについて」（P.8-23）
- 「アウトブレイク隔離」（P.8-23）

隔離内のメッセージの表示

目的	手順
隔離内のすべてのメッセージの表示	[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。 関連する隔離の行で、表の [メッセージ（Messages）] 列の青い番号をクリックします。
アウトブレイク隔離内のメッセージの表示	• [メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。 関連する隔離の行で、表の [メッセージ（Messages）] 列の青い番号をクリックします。 • 「[ルール サマリで管理（Manage by Rule Summary）] リンク」（P.8-24）を参照してください。
隔離内のメッセージのリストのナビゲート	[前へ（Previous）]、[次へ（Next）]、ページ番号、または二重矢印のリンクをクリックします。二重矢印を使用すると、リストの先頭（[<<]）または最後（[>>]）のページに移動します。
隔離内のメッセージのリストのソート	列見出しをクリックします（複数の項目が含まれる可能性のある列または [その他の隔離（In other quarantines）] 列を除く）。
表の列のサイズ変更	列見出し間のディバイダをドラッグします。
メッセージが隔離された原因のコンテンツの表示	「一致した内容の表示」（P.8-21）を参照してください。

隔離されたメッセージおよび国際文字セット

メッセージの件名に国際文字セット（2 バイト、可変長、および非 ASCII の符号化）の文字が含まれる場合、[ポリシー隔離（Policy Quarantine）] ページでは、非 ASCII 文字の件名行が復号化された形式で表示されます。

ポリシー、ウイルス、アウトブレイク隔離内メッセージの検索

（注）
- ポリシー、ウイルス、アウトブレイク隔離内の検索では、スパム隔離内のメッセージは見つかりません。
- ユーザは、ユーザがアクセスできる隔離内のメッセージだけを探して確認することができます。

手順

ステップ 1　[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 2　[複数の隔離を対象に検索（Search Across Quarantines）] ボタンをクリックします。

ヒント　アウトブレイク隔離では、アウトブレイク ルールによって隔離されたすべてのメッセージを検索することもできます。[アウトブレイク（Outbreak）] テーブル行の [ルール サマリで管理（Manage by Rule Summary）] リンクをクリックして、関連するルールをクリックします。

ステップ 3　検索を実施する隔離を選択します。

ステップ 4　（任意）他の検索条件を入力します。

- エンベロープ送信者およびエンベロープ受信者では、任意の文字を入力できます。入力の検証は実行されません。
- 検索結果には、指定した条件の *すべて* に一致するメッセージだけが含まれます。たとえば、エンベロープ受信者と件名を指定した場合は、エンベロープ受信者 *および* 件名両方で指定された条件に一致するメッセージだけが返されます。

次の作業

これらの検索結果は、隔離リストを使用するのと同様に使用できます。詳細については、「手動での隔離内のメッセージの処理」（P.8-19）を参照してください。

手動での隔離内のメッセージの処理

手動でメッセージを処理する場合は、[メッセージ アクション（Message Actions）] ページからメッセージのメッセージ アクションを手動で選択します。

（注）　RSA Enterprise Manager を使用する導入では、セキュリティ管理アプライアンス、または Enterprise Manager 上に隔離されたメッセージを表示できますが、メッセージでアクションを行うためには Enterprise Manager を使用する必要があります。Enterprise Manager の詳細については、電子メール セキュリティ アプライアンスのマニュアルの「Data Loss Prevention」の章を参照しください。

メッセージで次のアクションを行うことができます。

- 削除（Delete）
- リリース
- 隔離からの終了予定の遅延
- 指定した電子メール アドレスにメッセージのコピーを送信
- 1 つの隔離から別の隔離へのメッセージの移動

通常、次の作業を行うときに表示されるリスト内のメッセージ アクションを実施できます。ただし、すべての状況ですべてのアクションが使用可能なわけではありません。

- [メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] ページの隔離のリストから、隔離内のメッセージ数をクリックします。
- [複数の隔離を対象に検索（Search Across Quarantines）] をクリックします。
- 隔離の名前をクリックし、隔離内を検索します。

次に、複数のメッセージで次の操作を同時に実行できます。

- メッセージ リストの先頭の選択リストからオプションを選択する。
- ページ上の各メッセージの横のチェックボックスを選択する。
- メッセージ リストの先頭の表見出し内のチェックボックスを選択する。これで画面に表示されているすべてのメッセージにアクションが適用されます。他のページのメッセージは影響を受けません。

アウトブレイク隔離内のメッセージに対しては追加のオプションが利用可能です。電子メール セキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドの「Outbreak Filters」の章の [ルールサマリで管理（Manage by Rule Summary）] ビューについての情報を参照してください。

関連項目

- 「複数の隔離内のメッセージ」（P.8-20）
- 「自動的に処理される隔離メッセージのデフォルト アクション」（P.8-11）

メッセージのコピーの送信

メッセージのコピーは、管理者グループに属しているユーザだけが送信できます。

メッセージのコピーを送信するには、[コピーの送信先：（Send Copy To:）] フィールドに電子メールアドレスを入力し、[送信（Submit）] をクリックします。メッセージのコピーを送信しても、そのメッセージに対してその他のアクションが実行されることはありません。

ポリシー隔離間の移行メッセージについて

1 つのアプライアンス上で、1 つのポリシー隔離から別のポリシー隔離へ手動でメッセージを移動できます。

メッセージを別の隔離へ移動するには、次の手順に従ってください。

- 有効期限は変更されません。メッセージは、元の隔離の保留時間を維持します
- メッセージが隔離された原因は、コンテンツの一致やその他の関連する詳細も含め変更されません。
- メッセージが複数の隔離にあり、そのメッセージのコピーをすでに保留している宛先に移行する場合、メッセージの移動されるコピーの有効期限および隔離の原因が、宛先の隔離にもともとあるメッセージのコピーのそれらを上書きします。

複数の隔離内のメッセージ

メッセージが他の 1 つまたは複数の隔離内にある場合、隔離メッセージ リストの [その他の隔離（In other quarantines）] 列に、これらのほかの隔離にアクセスする許可があるかどうかに関係なく、[はい（Yes）] が表示されます。

複数の隔離内のメッセージ：

- 置かれていた隔離のすべてからメッセージがリリースされないかぎり配信されません。すべての隔離から削除されると、二度と配信できません。
- メッセージが置かれているすべての隔離から削除またはリリースされないかぎり、どの隔離からも削除されません。

メッセージをリリースしようとしているユーザがメッセージが置かれている隔離のすべてにアクセスできない可能性があるため、次のルールが適用されます。

- メッセージは、自身が存在するすべての隔離エリアから解放されるまで、どの隔離エリアからも解放されません。
- メッセージは、いずれかの隔離内で削除済みとマークされると、他の隔離からも配信できなくなります （ただし、リリースできます）。

したがって、メッセージが複数の隔離内にキューイングされ、ユーザがそのうちの 1 つまたは複数の隔離にアクセスできない場合は、次のことが起こります。

- ユーザは、ユーザがアクセスできる各隔離についてそのメッセージが存在するかどうか通知されます。
- GUI は、ユーザがアクセスできる隔離の保留期間の予定終了日時のみを表示します （同じメッセージに対して、隔離ごとに別々の終了日時が存在します）。
- ユーザは、そのメッセージを保管している他の隔離の名前を知らされません。
- ユーザは、ユーザがアクセス権限を持たない隔離にメッセージを置く原因となったコンテンツの一致を確認できません。
- メッセージのリリースは、ユーザがアクセスできるキューにだけ効果があります。
- ユーザがアクセスできない他の隔離にもメッセージがキューイングされている場合、残りの隔離にアクセスできるユーザによって処理されるまで（あるいは早期または通常の期限切れによって「正常に」リリースされるまで）、そのメッセージは変更されずに隔離内に残ります。

メッセージの詳細およびメッセージ コンテンツの表示

メッセージのコンテンツを表示したり、[隔離されたメッセージ（Quarantined Message）] ページにアクセスしたりするには、メッセージの件名行をクリックします。

[隔離されたメッセージ（Quarantined Message）] には、[隔離の詳細（Quarantine Details）] と [メッセージの詳細（Message Details）] の 2 つのセクションがあります。

[隔離されたメッセージ（Quarantined Message）] ページから、メッセージの読み取り、メッセージ アクションを選択したり、メッセージのコピーを送信したりできます。また、メッセージが隔離エリアから解放されるときに Encrypt on Delivery フィルタ アクションによって暗号化されるかどうかを確認することもできます。

[メッセージの詳細（Message Details）] セクションには、メッセージ本文、メッセージ ヘッダー、および添付ファイルが表示されます。メッセージ本文は最初の 100 KB だけが表示されます。メッセージがそれよりも長い場合は、最初の 100 KB が表示され、その後に省略記号（...）が続きます。実際のメッセージが切り捨てられることはありません。この処置は表示目的のためだけに行われます。[メッセージの詳細（Message Details）] の下部にある [メッセージ部分（Message Parts）] セクション内の

[message body] をクリックすることにより、メッセージ本文をダウンロードできます。また、添付ファイルのファイル名をクリックすることにより、メッセージの任意の添付ファイルをダウンロードすることもできます。

ウイルスの含まれるメッセージを表示する場合、ご使用のコンピュータにデスクトップ アンチウイルス ソフトウェアがインストールされていると、そのアンチウイルス ソフトウェアから、ウイルスが検出されたと警告される場合があります。これは、ご使用のコンピュータに対して脅威ではないため、無視しても問題ありません。

メッセージの詳細を表示するには、[メッセージ トラッキング（Message Tracking）] リンクをクリックします。

（注）　特別な Outbreak 隔離の場合、追加の機能を利用できます。「アウトブレイク隔離」（P.8-23）を参照してください。

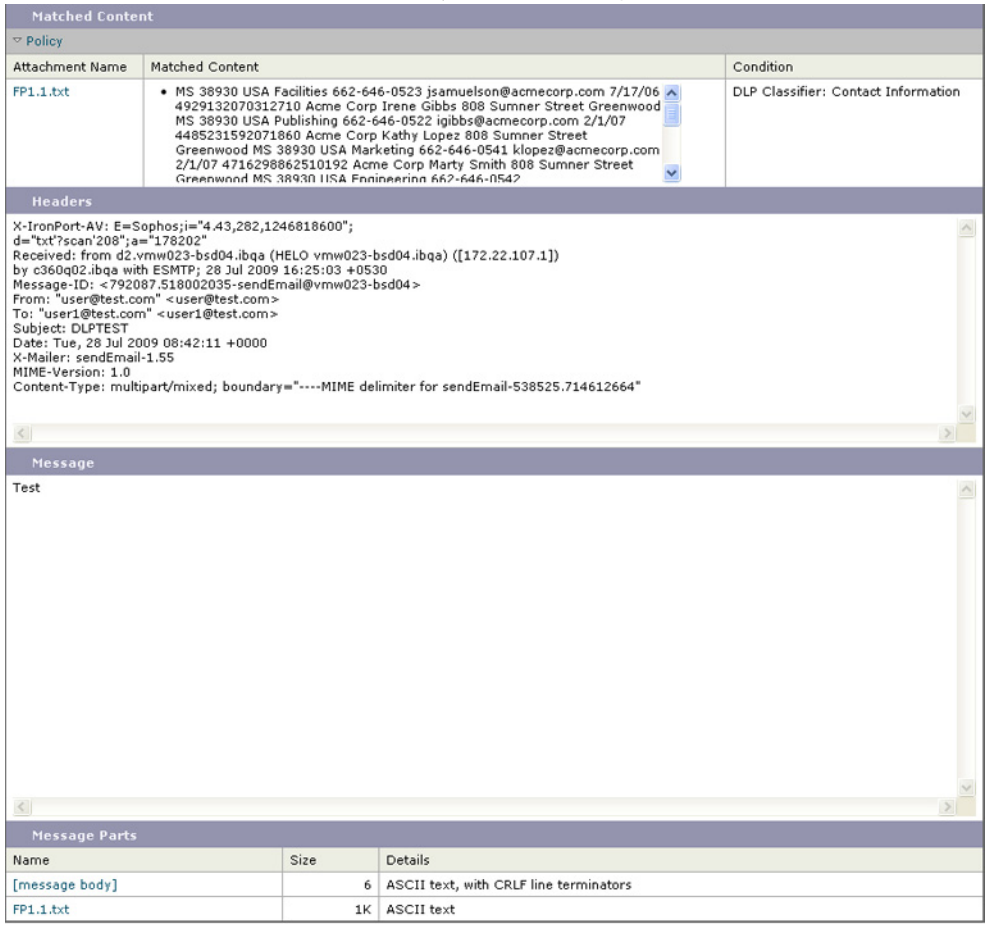
一致した内容の表示

Attachment Content 条件、Message Body または Attachment 条件、Message 本文条件、または Attachment 内容条件と一致するメッセージに対して隔離アクションを設定した場合、隔離されたメッセージ内の一致した内容を表示できます。メッセージ本文を表示する場合、DLP ポリシー違反の一致を除き、一致した内容が黄色で強調表示されます。また、$MatchedContent アクション変数を使用して、メッセージの一致した内容やコンテンツ フィルタの一致をメッセージの件名に含めることもできます。

一致した内容が添付ファイルに含まれる場合は、その判定結果が DLP ポリシー違反、コンテンツ フィルタ条件、メッセージ フィルタ条件、または画像解析のいずれによるものかに関係なく、添付ファイルの内容がその隔離理由とともに表示されます。

メッセージ フィルタまたはコンテンツ フィルタのルールをトリガーしたローカル隔離内のメッセージを表示すると、フィルタ アクションを実際にはトリガーしなかった内容が（フィルタ アクションをトリガーした内容とともに）GUI で表示されることがあります。GUI 表示は、内容の一致箇所を特定する際のガイドラインとして使用されますが、内容の一致リストを正確に反映しているとは限りません。これは、GUI で使用される内容一致ロジックが、フィルタで使用されるものほど厳密ではないため起こります。この問題は、メッセージ本文内での強調表示に対してのみ当てはまります。メッセージの各パート内の一致文字列をそれに対応するフィルタ ルールとともに一覧表示する表は正しく表示されます。

図 8-1　ポリシー隔離エリア内で表示された一致内容



添付ファイルのダウンロード

[メッセージ部分（Message Parts）] または [一致した内容：（Matched Content）] セクション内の添付ファイルのファイル名をクリックすることにより、メッセージの添付ファイルをダウンロードできます。AsyncOS から、未知の送信元からの添付ファイルにはウイルスが含まれる可能性があることを示す警告が表示され、続行するかどうか尋ねられます。ウイルスを含むかもしれない添付ファイルを自己責任においてダウンロードします。[メッセージ部分（Message Parts）] セクション内の `[message body]` をクリックすることにより、メッセージ本文をダウンロードすることもできます。

隔離されたメッセージの再スキャンについて

隔離内にあるキューすべてからメッセージがリリースされると、アプライアンスで使用可能な機能に基づきおよびメッセージが最初に隔離されたメール ポリシーに対して、次の再スキャンが開始されます。

- ポリシーおよびウイルス隔離からリリースされるメッセージはウイルス対策エンジンによって再スキャンされます。

- アウトブレイク隔離からリリースされるメッセージはスパム対策およびウイルス対策エンジンによって再スキャンされます（アウトブレイク隔離中のメッセージの再スキャンの詳細については、電子メール セキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドの「Outbreak Filters」の章を参照してください）。

再スキャンで、判定結果が前回そのメッセージを処理したときの判定結果と一致する場合、そのメッセージは再隔離されません。逆に、判定が異なると、そのメッセージは他の隔離に送信できます。

原理的に、メッセージの隔離が無限に繰り返されることはないようになっています。たとえば、メッセージが暗号化されていて、その結果、Virus 隔離に送信されるとします。管理者がそのメッセージをリリースしても、ウイルス対策エンジンはまだそのメッセージを復号化できません。しかし、そのメッセージは再隔離されない必要があるか、またはループ状態となりそのメッセージは二度と隔離からリリースされなくなります。2 回とも判定は同じ結果になるので、システムは 2 回めには Virus 隔離を無視します。

アウトブレイク隔離

アウトブレイク隔離は、アウトブレイク フィルタ機能の有効なライセンス キーが入力されている場合に存在します。アウトブレイク フィルタ機能では、しきい値セットに従ってメッセージがアウトブレイク隔離に送信されます。詳細については、の電子メール セキュリティ アプライアンスオンライン ヘルプまたはユーザ ガイドの「Outbreak Filters」の章を参照してください。

アウトブレイク隔離は、他の隔離と同じように運用され、メッセージの検索、メッセージのリリースまたは削除などができます。

アウトブレイク隔離には、他の隔離では使用できない追加の機能があります。これには、[ルール サマリで管理（Manage by Rule Summary）] リンク、メッセージの詳細を表示しているときの [シスコへ送信（Send to Cisco）] 機能、および [終了予定（Scheduled Exit）] の時間によって検索結果内のメッセージをソートするオプションがあります。

Outbreak フィルタ機能のライセンスの有効期限が切れると、メッセージをアウトブレイク隔離にそれ以上追加できなくなります。隔離エリア内に現在存在するメッセージの保存期間が終了してアウトブレイク隔離が空になると、GUI の隔離リストにアウトブレイク隔離は表示されなくなります。

アウトブレイク隔離内のメッセージの再スキャン

新しく発行されたルールによって、隔離されているメッセージがもう脅威ではないと考えられる場合にはアウトブレイク隔離に入れられたメッセージは自動的にリリースされます。

アプライアンス上でアンチスパムおよびアンチウイルスがイネーブルになっている場合、スキャン エンジンは、メッセージに適用されるメール フロー ポリシーに基づいて、アウトブレイク隔離から解放されたすべてのメッセージをスキャンします。

[ルール サマリで管理（Manage by Rule Summary）] リンク

隔離リストで Outbreak 隔離の横にある [ルール サマリで管理（Manage by Rule Summary）] リンクをクリックして、[ルール サマリで管理（Manage by Rule Summary）] ページを表示します。隔離エリア内のすべてのメッセージに対し、それらのメッセージを隔離させた感染防止ルールに基づいてメッセージ アクション（Release、Delete、Delay Exit）を実行できます。これは、アウトブレイク隔離から大量のメッセージを処理する場合に適しています。詳細については、電子メール セキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドの「Outbreak Filters」の章の [ルール サマリで管理（Manage by Rule Summary）] ビューについての情報を参照してください。

誤検出または疑わしいメッセージのシスコへのレポート

アウトブレイク隔離内のメッセージのメッセージ詳細を表示したときに、誤検出または疑わしいメッセージをレポートするためにこのメッセージをシスコに送信できます。

手順

ステップ 1　アウトブレイク隔離内のメッセージに移動します。

ステップ 2　[メッセージの詳細（Message Details）] セクションで、[シスコにコピーを送信する（Send a Copy to Cisco Systems）] チェックボックスを選択します。

ステップ 3　[送信（Send）] をクリックします。