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

この章は、次の項で構成されています。

集約隔離の概要

E メール セキュリティ アプライアンス上で特定のフィルタ、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隔離しておくことができます。Cisco コンテンツ セキュリティ管理アプライアンス上の複数の E メール セキュリティ アプライアンスから隔離を集約管理できます。

この集約隔離には次のような利点があります。

- 複数の E メール セキュリティ アプライアンスで隔離されたメッセージを 1 か所で管理できます。
- セキュリティ リスクを減らすため、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内側に保管されます。
- 集約隔離は、セキュリティ管理アプライアンスの標準バックアップ機能の一部としてバックアップされることができます。

ウイルス対策スキャン、アウトブレイク フィルタ、および高度なマルウェア防御（ファイル分析）には、それぞれ専用の隔離場所があります。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。

レガシー Web インターフェイスの [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）] セクションは、新しい Web インターフェイスでは [その他の隔離（Other Quarantines）] としてラベル付けされています。詳細については、隔離内のメッセージの表示 （25 ページ）を参照してください。

隔離の詳細については、お使いの E メール セキュリティ アプライアンスのドキュメントを参照してください。

隔離の種類

隔離タイプ	隔離名	デフォルトで作成される	説明	詳細情報
高度なマルウェア防御（Advanced Malware Protection）	ファイル分析（File Analysis）	○	判定が返されるまで、ファイル分析のために送信されたメッセージを保持します。	• ポリシー ブレイク • ポリシー ブレイク
ウイルス	ウイルス	○	アンチウイルス エンジンによる判定に従って、マルウェアを送信する可能性のあるメッセージを保持します。	
アウトブレイク	アウトブレイク	○	アウトブレイク フィルタでスパムまたはマルウェアの可能性があると検出されたメッセージを保持します。	
ポリシー	ポリシー	○	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用意されています。	
	Unclassified	○	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 アクションで指定した隔離が削除された場合にのみ、メッセージを保持します。 この隔離をフィルタやメッセージ アクションに割り当てることはできません。	
	（自分で作成する「ポリシー隔離」）	非対応	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」。	

隔離タイプ	隔離名	デフォルトで作成される	説明	詳細情報
スパム	スパム	○	スパムおよびその疑いのあるメッセージを保持して、メッセージの受信者や管理者が確認できるようにします。 スパム隔離は、ポリシー、ウイルス、およびアウトブレイクの隔離グループに含まれておらず、これらの隔離とは別に管理します。	スパム隔離

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

	コマンドまたはアクション	目的
ステップ 1	E メール セキュリティ アプライアンスが 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、これらのアプライアンスが集約されたポリシー、ウイルス、およびアウトブレイクの隔離データを交換できるようにファイアウォールのポートを開放する必要があります。	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上で、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有効化 （6 ページ）
ステップ 3	セキュリティ管理アプライアンスで、スパム以外の隔離に割り当てるディスク領域を指定します。	ディスク領域の管理
ステップ 4	（オプション） • セキュリティ管理アプライアンス上に、集約されたポリシー隔離を必要な設定で作成します。 • 集約するウイルス隔離とアウトブレイク隔離、およびデフォルトの「ポリシー隔離」を設定します。	• ポリシー、ウイルス、およびアウトブレイク隔離の設定 （15 ページ） • システム作成の隔離の設定を確認 （15 ページ）。

	コマンドまたはアクション	目的
	移行の前にこれらを設定済みの場合は、既存の設定を E メール セキュリティ アプライアンス上で参照できます。 カスタムの移行を設定するときに隔離を作成したり、自動移行時に隔離を自動作成したりできます。移行時に作成されるすべての隔離には、デフォルトの設定が適用されます。 ローカルの隔離の設定は、隔離名が同じでも集約隔離には継承されません。	
ステップ 5	セキュリティ管理アプライアンス上で、管理する E メール セキュリティ アプライアンスを追加するか、追加済みの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 E 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 E 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 E 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 （7 ページ）
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、E メール セキュリティ アプライアンスからの既存の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 （9 ページ）
ステップ 8	E 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機能を有効にします。 • **重要** E 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されます。	お使いのセキュリティ管理アプライアンスのマニュアルで、「Centralizing Services on a Cisco Content Security Management appliance」の章の以下の項を参照してください。 • 「About Migration of Policy, Virus, and Outbreak Quarantines」 • 「ポリシー、ウイルス、およびアウトブレイク隔離の集約（Centralizing Policy, Virus, and Outbreak Quarantines）」

	コマンドまたはアクション	目的
ステップ 9	追加の E メール セキュリティ アプライアンスを移行します。 • 同時に移行できるのは 1 つのアプライアンスのみです。前の移行が完了する前に、別の E 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の集約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。 • 移行時に作成される隔離には、隔離名が同じでも、元のローカルの隔離での設定ではなくデフォルトの設定が適用されます。	ポリシー、ウイルス、およびアウトブレイク隔離の設定 （15 ページ）
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されない場合は、E メール セキュリティ アプライアンス上でこれらの設定を手動で更新する必要があります。 • クラスタ構成では、フィルタおよびメッセージ アクションが特定のレベルで定義されている場合に限り、それらの設定がそのレベルで自動的に更新されます。	詳しくは、お使いの E 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 アクションについての説明を参照してください。
ステップ 12	（推奨）元の E メール セキュリティ アプライアンスが使用できない場合に備えて、隔離からリリースされたメッセージを処理する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 （11 ページ）
ステップ 13	カスタム ユーザ ロールに管理タスクを委任する場合は、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

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有効化

始める前に

ポリシー、ウイルス、およびアウトブレイク隔離の集約 （4 ページ）の表に記載されているここまでの手順を完了してください。

ステップ 1 [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）] の順に選択します。

ステップ 2 [有効（Enable）] をクリックします。

ステップ 3 E 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。
- 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。
- ファイアウォールで開放したポートを使用する必要があります。

ステップ 4 [送信（Submit）] をクリックします。

次のタスク

ポリシー、ウイルス、およびアウトブレイク隔離の集約 （4 ページ）の表に戻り、次のステップに進みます。

アプライアンスの新しいWebインターフェイ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有効化

始める前に

ポリシー、ウイルス、およびアウトブレイク隔離の集約 （4 ページ）の表に記載されているここまでの手順を完了してください。

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、 [その他の隔離（Other Quarantine）] に対応する アイコンにカーソルを合わせて、[設定の編集（Edit Settings）] をクリックします。

ステップ 2 レガシーインターフェイスにリダイレクトされたら、[有効（Enable）] をクリックします。

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 E メール セキュリティ アプライアンスで、すべての隔離の統合されたビューを表示するには、隔離を集中化する前に、すべての E メール セキュリティ アプライアンスの追加を検討します。

始める前に

ポリシー、ウイルス、およびアウトブレイク隔離の集約 （4 ページ）の表に記載されているここまでの手順を完了してください。

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。

a) 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。

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 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。

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）] フィールドに、追加するアプライアンス名前と管理インターフェイスの 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 名を入力しても、[送信（Submit）] をクリックすると IP アドレスに変換されます。

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フレーズを入力し、[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。

f) 「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 5 **[送信（Submit）]** をクリックします。

ステップ 6 [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 E メール セキュリティ アプライアンスについてこの手順を繰り返します。

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 7 変更を保存します。

次のタスク

ポリシー、ウイルス、およびアウトブレイク隔離の集約 （4 ページ）の表に戻り、次のステップに進みます。

ポリシー、ウイルス、アウトブレイク隔離の移行の設定

始める前に

- 次の項の表に記載されているここまでの手順を完了してください。ポリシー、ウイルス、およびアウトブレイク隔離の集約 （4 ページ）
- 移行プロセスに関する警告や情報については、お使いの E 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 Security Management appliance」の章の「About Migration of Policy, Virus, and Outbreak Quarantines」の項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）] の順に選択します。

ステップ 3 [移行ウィザードを起動（Launch Migration Wizard）] をクリックします。

ステップ 4 移行方法を選択します。

条件（IF）	移行方法	その他の情報
• 関連付けられているすべての E メール セキュリティ アプライアンスから既存のすべての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がすべての E メールセキュリティアプライアンス上で同一設定である場合 および • すべての E メール セキュリティ アプライアンスから同名のすべてのポリシー隔離を同名の単一のポリシー隔離に集約する場合	[自動（Automatic）]	この移行方法で作成されるすべての集約されたポリシー隔離には、E メール セキュリティ アプライアンスの同名の隔離の設定に関係なく、デフォルトの設定が適用されます。 移行後に、これらの設定を更新する必要があります。

条件（IF）	移行方法	その他の情報
• 複数の E メール セキュリティ アプライアンス上で同名のポリシー隔離の設定が異なっており、この違いを保持したまま移行する場合 または • ローカル隔離の一部を移行し、他のすべてを削除する場合 または • ローカル隔離を別名の集約隔離に移行する場合 または • 異なる名前のローカル隔離を単一の集約隔離にマージする場合	カスタム（Custom）	移行前ではなく移行時に作成するすべての集約されたポリシー隔離には、新しい隔離用のデフォルトの設定が適用されます。 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 5 [Next] をクリックします。

ステップ 6 [自動（Automatic）] を選択した場合は、次の手順に従います。

移行するポリシー隔離およびこのページの他の情報を確認します。

ウイルス、アウトブレイク、およびファイル分析の隔離も移行されます。

ステップ 7 [カスタム（Custom）] を選択した場合は、次の手順に従います。

- [隔離の表示元（Show Quarantines from）] リストで、すべての E メール セキュリティ アプライアンスの隔離を表示するか、特定のアプライアンスの隔離を表示するかを選択します。
- 各集約されたポリシー隔離に移行するローカルのポリシー隔離を選択します。
- 必要に応じて、追加の集約された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 E メール セキュリティ アプライアンスから削除されます。
- 隔離のマッピングを変更するには、右のテーブルで隔離を選択し、 [集約隔離から削除（Remove from Centralized Quarantine）] をクリックします。

ステップ 8 必要に応じて [次へ（Next）] をクリックします。

ステップ 9 変更を送信し、保存します。

次のタスク

ポリシー、ウイルス、およびアウトブレイク隔離の集約 （4 ページ）の表に戻り、次のステップに進みます。

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、セキュリティ管理アプライアンスによりそのメッセージが元のEメールセキュリティアプライアンスに返され、そこで処理されます。

元の E メール セキュリティ アプライアンスが使用できない場合は、リリースされたメッセージを別の E 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。この目的で使用するアプライアンスを指定します。

始める前に

- 代替アプライアンスが、リリースされたメッセージの処理および配信に適しているかどうかを確認します。たとえば、暗号化とアンチウイルス再スキャンの設定が、元のアプライアンスの設定と同じである必要があります。
- 代替アプライアンスは、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用に正しく設定されている必要があります。そのアプライアンスについて、ポリシー、ウイルス、およびアウトブレイク隔離の集約 （4 ページ）の表の手順を実行します。

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 [フォールバック ホスト アプライアンスを指定（Specify Alternate Release Appliance）] ボタンをクリックします。

ステップ 4 E メール セキュリティ アプライアンスを選択します。

ステップ 5 変更を送信し、保存します。

次のタスク

関連項目

E メール セキュリティ アプライアンスを使用できないときのメッセージのリリース （12 ページ）

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 E 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されたポリシー隔離

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 E 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

中央集中型のポリシー、ウイルス、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場合は、E メール セキュリティ アプライアンス上で行います。

ポリシー、ウイルス、およびアウトブレイク隔離の集約を無効にした場合の影響など、詳細については、お使いの E 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。

Eメールセキュリティアプライアンスを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、セキュリティ管理アプライアンスによりそのメッセージが元のEメールセキュリティアプライアンスに返され、そこで処理されます。

元の E メール セキュリティ アプライアンスが使用できない場合は、リリースされたメッセージを別の E 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。この目的で使用する代替アプライアンスを指定します。

代替アプライアンスが使用できない場合は、代替リリース アプライアンスとして別の E 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。

E メール セキュリティ アプライアンスへのアクセスに繰り返し失敗すると、アラートが送信されます。

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 （11 ページ）

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へのディスク領域の割り当て （13 ページ）
- 隔離内のメッセージの保持期間 （13 ページ）
- 隔離メッセージに自動的に適用されるデフォルト アクション （15 ページ）
- システム作成の隔離の設定を確認 （15 ページ）

ポリシー、ウイルス、およびアウトブレイク隔離への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、ディスク領域の管理を参照してください。

複数の隔離のメッセージは、1つの隔離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。

- ローカルのポリシー隔離、ウイルス隔離、およびアウトブレイク隔離に割り当てられるべきアプライアンス上のすべてのディスク領域が、アウトブレイク隔離内のメッセージのコピーを保持するために使用されます。これらのメッセージは、アウトブレイクルールが更新されるたびにスキャンされます。
- 特定の管理対象電子メール セキュリティ アプライアンスから隔離された、アウトブレイク隔離内のメッセージに使用できるセキュリティ管理アプライアンスのディスク領域は、その電子メール セキュリティ アプライアンスで隔離メッセージに使用できるディスク領域の量によって制限される場合があります。
- この状況の詳細については、次を参照してください。 隔離内のメッセージの保持期間 （13 ページ）

関連項目

- 隔離のステータス、容量、およびアクティビティのモニタリング （21 ページ）
- 隔離用のディスク容量の使用率に関するアラート （23 ページ）
- 隔離内のメッセージの保持期間 （13 ページ）

隔離内のメッセージの保持期間

メッセージは次のタイミングで隔離から自動的に削除されます。

- 通常の期限切れ：隔離エリア内のメッセージが設定された保存期間を満了した場合です。各隔離エリアのメッセージの保存期間を指定します。各メッセージには一定の保持期間があり、その期間のみ隔離の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い限り、メッセージは指定された期間が経過するまで保持されます。

（注） アウトブレイク フィルタ隔離でのメッセージの通常の保持期間は、アウトブレイク隔離ではなく各メールのアウトブレイク フィルタ セクションで設定します。

- 早期の期限切れ：設定した保持期間が経過する前にメッセージが隔離から強制的に削除された場合です。これは次の場合に発生します。
  - ポリシー、ウイルス、およびアウトブレイク隔離へのディスク領域の割り当て （13 ページ）で定義した、すべての隔離に対するサイズ制限に達した場合。

    サイズ制限に達すると、隔離に関係なく、古いメッセージからデフォルトアクションが適用されます。すべての隔離のサイズが制限値未満に戻るまで、各メッセージに対してデフォルトアクションが実行されます。このポリシーは、First In First Out（FIFO; 先入れ先出し）です。複数の隔離内に保持されたメッセージの場合は、最新の保持期間に基づいて期限切れになります。

    （任意）ディスク容量が不足したときのリリースまたは削除の対象から、特定の隔離を除外することができます。除外するようにすべての隔離を設定して、ディスク領域が満杯になった場合、。

    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 E メール セキュリティ アプライアンスに保存されます。これにより、E 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内のメッセージを再スキャンし、安全と判断したメッセージをリリースするようセキュリティ管理アプライアンスに通知できます。アウトブレイク隔離の両方のコピーは常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、E 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、早く期限切れになります。

    ディスク領域の容量が一定の値に達すると、アラートが送信されます。隔離用のディスク容量の使用率に関するアラート （23 ページ）を参照してください。

- メッセージを保持している隔離を削除した場合。

メッセージが隔離から自動的に削除されるときに、そのメッセージに対してデフォルト アクションが実行されます。隔離メッセージに自動的に適用されるデフォルト アクション （15 ページ） を参照してください。

（注） これらのシナリオに加えて、スキャン操作の結果に基づいて、メッセージを隔離から自動的に削除できます（アウトブレイク フィルタまたはファイル分析）。

保存期間への時間調整の影響

- サマータイムとアプライアンス のタイムゾーンの変更は保持期間に影響しません。
- 隔離の保持期間を変更すると、その保持期間は新しいメッセージにのみ適用され、既存のメッセージには適用されません。
- システム クロックを変更してメッセージの保持期間が過ぎた場合は、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の処理中のメッセージには適用されません。

隔離メッセージに自動的に適用されるデフォルト アクション

隔離内のメッセージの保持期間 （13 ページ）に記述されるいずれかの状況が発生した場合、ポリシー、ウイルス、またはアウトブレイク隔離内のメッセージに対してデフォルトアクションが実行されます。

デフォルト アクションには、以下の 2 つがあります。

- 削除：メッセージを削除します。
- リリース：メッセージが解放されて配信されます。

メッセージのリリース時に、脅威に対する再スキャンが実行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 （32 ページ）を参照してください。

また、指定した保持期間よりも前にリリースされるメッセージには、X-Headerの追加などの操作が行われる場合があります。詳細については、ポリシー、ウイルス、およびアウトブレイク隔離の設定 （15 ページ）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元の E メール セキュリティ アプライアンス に返され、そこで処理されます。

システム作成の隔離の設定を確認

隔離を使用する前に、デフォルトの隔離設定（未分類隔離など）をカスタマイズします。

関連項目

- ポリシー、ウイルス、およびアウトブレイク隔離の設定 （15 ページ）

ポリシー、ウイルス、およびアウトブレイク隔離の設定

始める前に

- 既存の隔離を編集する場合は、ポリシー、ウイルス、およびアウトブレイク隔離の設定の編集について （18 ページ）を参照してください。
- 保持期間やデフォルトアクションなど、隔離内のメッセージを自動的に管理する方法を確認します。隔離内のメッセージの保持期間 （13 ページ）および隔離メッセージに自動的に適用されるデフォルト アクション （15 ページ）を参照してください。

- 各隔離にアクセスできるユーザを決め、ユーザおよびカスタム ユーザ ロールを作成します。詳細は、ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザ グループの指定 （24 ページ）を参照してください。

ステップ 1 ポリシー、ウイルス、およびアウトブレイク隔離は、次のいずれかの方法で設定できます。

- （新しい Web インターフェイスのみ）[隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）] > [+] を選択します。
- [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、次のいずれかを実行します。
  - [ポリシー隔離の追加（Add Policy Quarantine）] をクリックします。
  - 編集する隔離をクリックします。

ステップ 2 次の情報を入力します。

次の点を考慮してください。

- ファイル分析隔離の保持期間をデフォルトの 1 時間から変更することは推奨されません。
- 隔離ディスク領域が一杯になった場合でも、指定した保存期間の終了前にこの隔離メッセージを処理されたくない場合、[メッセージに対してデフォルトのアクションを適用して空き容量を増やす（Free up space by applying default action on messages upon space overflow）] の選択を解除します。

  このオプションはすべての隔離では選択しないでください。システムは、少なくとも 1 つの隔離エリアからメッセージを削除して、領域を確保する必要があります。
- デフォルト アクションとして [リリース（Release）] を選択すると、保持期間前にリリースされるメッセージに適用する追加の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）	追加するテキストを入力し、そのテキストを元の件名の前と後ろのどちらに追加するかを選択します。 たとえば、受信者に不適切なコンテンツを含む可能性があるメッセージであることを警告するテキストを追加します。 （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 の追加（Add X-Header）]	X-Header にはメッセージに対して実行されたアクションを記録できます。この情報は、特定のメッセージが配信された理由についての照会を処理するときなどに役立ちます。 名前と値を入力します。 例： Name = Inappropriate-release-early Value = True
添付ファイルを除去（Strip Attachments）	添付ファイルを除去すると、そのファイルに存在する潜在的なウイルスから保護できます。

ステップ 3 この隔離へのアクセスを付与するユーザーを指定します。

ユーザー	情報
ローカル ユーザー（Local Users）	ローカル ユーザーのリストには、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完全なアクセス権限を持つため、リストでは管理者が除外されます。
外部認証されたユーザー（Externally Authenticated Users）	外部認証を設定しておく必要があります。
カスタムユーザーロール（Custom User Roles）	このオプションは、隔離へのアクセス権限を持つ少なくとも 1 つのカスタム ユーザー ロールを作成している場合にのみ表示されます。

ステップ 4 変更を送信し、保存します。

次のタスク

[メッセージフィルタ（Message Filters）] ページおよび[コンテンツフィルタ（Content Filters）] ページを参照してください。

- まだ E 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は、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、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。

  メッセージを隔離するためのメッセージ フィルタ、コンテンツ フィルタ、および DLP メッセージ アクションが E メール セキュリティ アプライアンスに定義されていることを

確認します。詳しくは、E 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、およびアウトブレイク隔離の設定の編集について

（注）
- 隔離の名前は変更できません。
- 隔離内のメッセージの保持期間 （13 ページ）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。

新しい Web インターフェイスで隔離の設定を変更するには、[隔離（Quarantine）]>[その他の隔離（Other Quarantine）]>[表示（View）] に移動し、必要な隔離で をクリックします。

レガシー Web インターフェイスで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。

ポリシー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

ポリシー隔離に関連付けられているメッセージ フィルタ、コンテンツ フィルタ、データ損失の防止（DLP）メッセージアクション、DMARC検証プロファイル、およびそれぞれが設定されている E メール セキュリティ アプライアンスを表示できます。

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）]>[その他の隔離（Other Quarantine）]>[表示（View）] をクリックします。

ステップ 2 （新しい Web インターフェイスのみ）必要な隔離を選択して ボタンをクリックします。

ステップ 3 [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 4 ポリシー隔離の名前をクリックします。

ステップ 5 ページの下部までスクロールし、[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）] を確認します。

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、アクティブなフィルタやメッセージアクションに関連付けられているかどうかを確認します。ポリシー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 （18 ページ）を参照してください。
- フィルタやメッセージアクションが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、ディスクがいっぱいになった際にメッセージを削除しないオプションを選択した場合でも、隔離で定義されたデフォルトアクションはすべてのメッセージに適用されます。隔離メッセージに自動的に適用されるデフォルト アクション （15 ページ）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関連付けられた隔離を削除した後でそのフィルタまたはメッセージ アクションにより隔離されたメッセージは、未分類隔離に格納されます。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しておく必要があります。
- 未分類隔離は削除できません。

PVO 検疫しきい値アラート

Cisco Secure Email and Web Manager では、PVO 検疫メッセージの数が、特定の期間と PVO 検疫に対して設定されたユーザー定義のしきい値を超えると、受信者にアラートが送信されます。Cisco Secure Email and Web Manager を使用すると、電子メールとして設定したアラートを受信できます。

CLI または Web インターフェイスを使用して、PVO 隔離しきい値アラートを設定できます。

関連項目

- CLI を使用した PVO の隔離しきい値アラート設定 （19 ページ）
- Web インターフェイス を使用した PVO の隔離しきい値アラート設定 （20 ページ）

CLI を使用した PVO の隔離しきい値アラート設定

PVO 隔離しきい値アラートを設定するには、CLI で `quarantineconfig` コマンドを使用します。コマンドを実行すると、PVO 隔離しきい値アラートを有効または無効にするように求められます。デフォルトでは、PVO 隔離しきい値アラートは無効になっています。次のパラメータの値を指定する必要があります。

- **しきい値**：しきい値を設定します。PVO 隔離メッセージの数がこの値を超えると、Secure Email および Web Manager は受信者にアラートを送信します。この値は、隔離ポリシーごとに設定できます。値の範囲は 1 ～ 10,00,000 です。
- **期間**：Secure Email および Web Manager が各隔離の PVO 隔離メッセージの数をカウントする必要がある期間（時間単位）を設定します。値の範囲は 0.5 ～ 24 です。期間の値は、0.5 の倍数（0.5、1、1.5 など）でのみ設定できます。

- **アラート制限**：アラート制限を設定します。この値は、設定された期間中に Secure Email および Web Manager が受信者に送信するアラートの数を示します。この値は、隔離ポリシーごとに設定されます。値の範囲は 1 ～ 20 です。

手順

コマンドまたはアクション	目的
`quarantineconfig`	PVO の隔離しきい値アラートを設定します。

Web インターフェイス を使用した PVO の隔離しきい値アラート設定

Secure Email および Web Manager の Web インターフェイスを使用して、PVO 隔離しきい値アラートを設定できます。

始める前に

PVO隔離しきい値アラートを受信するには、次の前提条件を満たしていることを確認してください。

- システムアラートが設定されている。
- 有効なシステム：クリティカルアラート。

ステップ 1 （新しい Web インターフェイスのみ）⚙ で Secure Email および Web Manager 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 [電子メール（Email）] > [メッセージの隔離（Message Quarantines）] > [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）] ページに移動します。

[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）] ページが表示されます。[隔離（Quarantines）] ウィンドウに、すべての PVO 隔離が表示されます。

ステップ 3 [ポリシー隔離の追加（Add Policy Quarantine）] をクリックして新しいPVO隔離を追加するか、既存のPVO隔離をクリックして PVO 隔離を編集します。

PVO 隔離の追加と編集の詳細については、ポリシー、ウイルス、およびアウトブレイク隔離の設定 （15 ページ）セクションを参照してください。

ステップ 4 [しきい値アラート設定（Threshold Alert Settings）] ウィンドウで、[しきい値アラートを有効にする（Enable Threshold Alert）] チェックボックスをオンにします。

ステップ 5 [しきい値アラート設定（Threshold Alert Settings）] ウィンドウの次のフィールドに値を入力します。

- [しきい値（Threshold）]
- [期間（Time Duration）]
- [アラート制限（Alert Limit）]

これらのパラメータ値の詳細については、CLIを使用したPVOの隔離しきい値アラート設定（19ページ）セクションを参照してください。

ステップ6 変更を送信し、保存します。

隔離のステータス、容量、およびアクティビティのモニタリング

目的	操作手順
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	（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。 **[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、そのページの最初のセクションを確認します。 割り当ての変更方法については、ディスク領域の管理を参照してください。
スパム隔離以外のすべての隔離で使用可能な領域を確認する	（新しいWebインターフェイスのみ）[隔離（Quarnatine）] > [その他の隔離（Other Quarantine）] を選択します。 または **[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、テーブルのすぐ下で確認します。 ポリシー、ウイルス、アウトブレイク隔離のために使用可能な領域が [隔離（Quarantines）] セクションの表の上に表示されます。
現在すべての隔離が使用している合計容量を確認する	（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。 [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。

目的	操作手順
現在各隔離に使用されている容量を確認する	（新しい Web インターフェイスのみ）[隔離（Quarantines Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）] を選択します。 この表には、各隔離で現在使用されている容量が表示されます。 または **[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。
現在すべての隔離にあるメッセージの総数を確認する	（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。 [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。
現在各隔離にあるメッセージ数を確認する	（新しい Web インターフェイスのみ）[隔離（Quarantines Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）] を選択します。 この表には、各隔離で現在使用可能なメッセージの総数が表示されます。 または [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、テーブル行でその隔離を確認します。
すべての隔離による総 CPU 使用率を確認する	（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。 [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。

目的	操作手順
最後のメッセージが各隔離に送信された日時（ポリシー隔離間の移動を除く）を確認する	（新しい Web インターフェイスのみ）**[隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）]** を選択します。 この表には、最後のメッセージが隔離された日時が表示されます。 または [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、テーブル行でその隔離を確認します。
ポリシー隔離が作成された日時を確認する ポリシー隔離の作成者の名前	（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。 **[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。
ポリシー隔離に関連付けられたフィルタおよびメッセージ アクションを確認する	ポリシー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 （18 ページ） 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、およびアウトブレイク隔離の合計容量が 75%、85%、および 95% になると、アラートが送信されます。使用率は、メッセージが隔離内に格納されたときにチェックされます。たとえば、メッセージが隔離に追加されたときに隔離エリアの合計サイズが指定容量の 75% 以上に増加すると、アラートが送信されます。

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)

そのメッセージを隔離したメッセージ フィルタまたはアウトブレイク フィルタ機能のルールがかっこ内に出力されます。メッセージを格納する隔離ごとに個別のログエントリが生成されます。

また、隔離から削除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)

すべての隔離から削除されたメッセージが完全に削除されたり配信がスケジュールされたりすると、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。これは、次のように新しい MID「by 行」がある既存のログ 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割り当てについて

メッセージの処理および確認タスクを、他の管理者ユーザに割り当てることができます。次に例を示します。

- 人事部門ではポリシー隔離の確認と管理を行います。
- 法務部門では Confidential Material 隔離を管理します。

隔離の設定を指定するときに、これらの部門のユーザにアクセス権限を割り当てます。隔離のアクセス権限は、既存のユーザのみに割り当てることができます。

すべてまたは一部の隔離へのアクセスを付与したり、すべての隔離にアクセスできないようにしたりできます。隔離を閲覧するための権限が付与されていないユーザには、GUI または CLI の隔離リストにその隔離が表示されません。

関連項目

- ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザ グループの指定（24 ページ）
- 管理タスクの分散

ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザグループの指定

管理ユーザに隔離へのアクセスを許可した場合、実行できるアクションはそのユーザ グループにより異なります。

- 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 ユーザ グループに属するユーザに加え、隔離管理権限を持つカスタム ユーザ ロールのユーザは、隔離エリア内のメッセージの検索、閲覧および処理が可能ですが、隔離の設定変更、作成、削除、または集約はできません。各隔離にどのユーザがアクセスできるかを指定できます。

• 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。

また、メッセージ トラッキングおよびデータ消失防止など、関連機能のアクセス権限により、[隔離（Quarantine）]ページに表示されるオプションおよび情報が異なります。たとえば、メッセージ トラッキングにアクセスできないユーザの場合、そのユーザにはメッセージ トラッキング、隔離されたメッセージに関する情報が表示されません。

注：セキュリティ管理アプライアンスで設定したカスタムユーザ 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方法については、カスタムユーザ ロールの集約隔離アクセスの設定 （11 ページ）を参照してください。

エンドユーザは、ポリシー、ウイルス、およびアウトブレイク隔離を閲覧したりアクセスしたりすることはできません。

ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作

関連項目

- 隔離内のメッセージの表示 （25 ページ）
- ポリシー、ウイルス、およびアウトブレイク隔離でのメッセージの検 （27 ページ）
- 隔離内のメッセージの手動処理 （28 ページ）
- 複数の隔離内にあるメッセージ （29 ページ）
- メッセージの詳細およびメッセージ内容の表示 （30 ページ）
- 隔離されたメッセージの再スキャンについて （32 ページ）
- アウトブレイク隔離 （33 ページ）

隔離内のメッセージの表示

目的	操作手順
隔離のすべてのメッセージを表示する	（新しい Web インターフェイスのみ）[隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）] を選択します。 または [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）] を選択します。 テーブル内の隔離の行で、[メッセージ（Messages）] 列の青い番号をクリックします。

目的	操作手順
アウトブレイク隔離エリアのメッセージを表示する	（新しい Web インターフェイス）[隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）] を選択します。 または [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）] を選択します。 テーブル内の隔離の行で、[メッセージ（Messages）] 列の青い番号をクリックします。 [ルール サマリー管理（Manage by Rule Summary）] リンク （34 ページ）またはルール サマリー ビュー （34 ページ）（新しい Web インターフェイスのみ）を参照してください。
隔離のメッセージのリスト表示を移動する	[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。 （新しい Web インターフェイスのみ）すべての新しいメッセージの詳細を表示するには、テーブルを下方向にスクロールします。
隔離エリアのメッセージのリストをソートする	列見出しをクリックします（列に複数の項目が含まれる場合と [その他の隔離（In other quarantines）]列を除く）。
テーブルの列サイズを変更する	列見出し間の境界線をドラッグします。
テーブル カラムのカスタマイズ	をクリックして、表示する列を選択し、[閉じる（Close）] をクリックします
メッセージの隔離の原因となったコンテンツを表示する	一致した内容の表示 （31 ページ） を参照してください。

関連項目

- 隔離されたメッセージおよび国際文字セット （26 ページ）

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 エンコーディング）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されて表示されます。

ポリシー、ウイルス、およびアウトブレイク隔離でのメッセージの検

（注）
- ユーザは、アクセス権限が付与された隔離内のメッセージだけを検索および表示できます。
- ポリシー、ウイルスおよびアウトブレイク隔離の検索では、スパム隔離内のメッセージは見つかりません。

ステップ 1 （新しい Web インターフェイスのみ）[隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [検索（Search）] 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）該当する隔離の青い番号のリンクをクリックします。

ヒント （新しいWebインターフェイスのみ）アウトブレイク隔離では、各アウトブレイク ルールにより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。アウトブレイク隔離で[ルールサマリー（Rule Summary）] タブをクリックして、関連するルールをクリックします。

ステップ 3 **[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 4 [隔離全体を検索（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、各アウトブレイク ルールにより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 テーブル行で [ルールサマリー管理（Manage by Rule Summary）] リンクをクリックします

ステップ 5 （任意）他の検索条件を入力します。

- [エンベロープ送信者（Envelope Sender）] および [エンベロープ受信者（Envelope Recipient）] には任意の文字を入力できます。エントリ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（Envelope Recipient）] および [件名（Subject）] を指定した場合は、[エンベロープ受信者（Envelope Recipient）] および [件名（Subject）] に指定した条件の両方に一致するメッセージだけが検索結果として表示されます。

次のタスク

これらの検索結果は、隔離のリストと同じように操作できます。詳細については、隔離内のメッセージの手動処理 （28 ページ）を参照してください。

検索条件の変更については、検索条件の変更 （28 ページ） を参照してください。

検索条件の変更

検索条件をカスタム時間範囲または別の隔離に変更できます。

検索条件を変更するには、[変更（Modify）] をクリックします。

隔離内のメッセージの手動処理

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 アクションを選択します。

メッセージに対し、次の処理を実行できます。

- 削除
- リリース
- 隔離からの予定していた終了の遅延
- 指定した電子メール アドレスへのメッセージのコピーの送信
- 別の隔離へのメッセージの移動

通常、以下の状況でリストのメッセージを処理できます。ただし、すべての状況ですべてのアクションが使用できる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）]** ページまたは（新しいWebインターフェイスのみ）**[隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）]** 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。
- 隔離メッセージのチェックボックスをオンにし、必要な操作を選択します。

複数のメッセージに同時にアクションを実行するには、次の操作を行います。

- メッセージ リストの上部の選択リストからオプションを選択する。
- ページ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上部のテーブル見出しでチェックボックスを選択する。これにより、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のメッセージのみに実行できるオプションもあります。*E*メールセキュリティ アプライアンスの *AsyncOS* 向けのオンライン ヘルプまたはユーザ ガイドの「Outbreak Filters」の章の [ルールサマリーによる管理（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

- メッセージのコピーの送信 （29 ページ）

- ポリシー隔離間のメッセージの移動について （29 ページ）
- 複数の隔離内にあるメッセージ （29 ページ）
- 隔離メッセージに自動的に適用されるデフォルト アクション （15 ページ）

メッセージのコピーの送信

メッセージのコピーは、Administrators 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。

ポリシー隔離間のメッセージの移動について

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。

別の隔離にメッセージを移動する場合次のようになります。

- 有効期限は変更されません。メッセージには、元の隔離での保持期限が適用されます。
- 一致したコンテンツおよび他の関連情報を含め、メッセージの隔離理由は変更されません。
- あるメッセージが複数の隔離にあり、すでにメッセージのコピーを保持している場所にメッセージを移動した場合、移動したメッセージのコピーの有効期限および隔離の理由は、移動先の隔離エリアに元からあるメッセージのコピーを上書きします。

複数の隔離内にあるメッセージ

同じメッセージが複数の隔離内に格納されている場合、これらの隔離へのアクセス権限があるかどうかにかかわらず、隔離メッセージ リストの [その他の隔離（In other quarantines）] 列に [はい（Yes）] が表示されます。

複数の隔離内にメッセージが格納されている場合、以下の点に注意してください。

- すべての隔離からリリースされるまで、そのメッセージは配信されません。いずれかの隔離から削除されたメッセージは配信されなくなります。
- すべての隔離から削除またはリリースされるまで、そのメッセージはいずれの隔離からも削除されません。

複数の隔離内に格納されているメッセージをリリースする場合、それらのすべての隔離に対するアクセス権限が付与されていない場合があるため、次のルールが適用されます。

- すべての隔離からリリースされるまで、そのメッセージはリリースされません。
- いずれかの隔離内で削除済みとしてマークされると、他の隔離からも配信できなくなります（ただしリリースは可能です）。

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、次の処理が行われます。

- 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。
- ユーザがアクセスできる隔離での保持期間の情報のみが GUI に表示されます（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。
- メッセージの隔離先にユーザがアクセスできない場合、その隔離理由は表示されません。
- ユーザがアクセスできるキューのメッセージのみリリースできます。
- 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、それら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」メッセージが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内容の表示

メッセージの内容を表示したり、[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）] ページには、[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、メッセージを読んだり、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、。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 K 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 K 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、メッセージの添付ファイルをダウンロードすることもできます。

（注） [メッセージの詳細（Message Details）] ページの添付ファイルのダウンロードの上限は 25 MB に制限されています。

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。

（注） 特別な Outbreak 検疫の場合、追加の機能を利用できます。アウトブレイク隔離 （33 ページ）を参照してください。

関連項目

- 一致した内容の表示 （31 ページ）
- 添付ファイルのダウンロード （32 ページ）

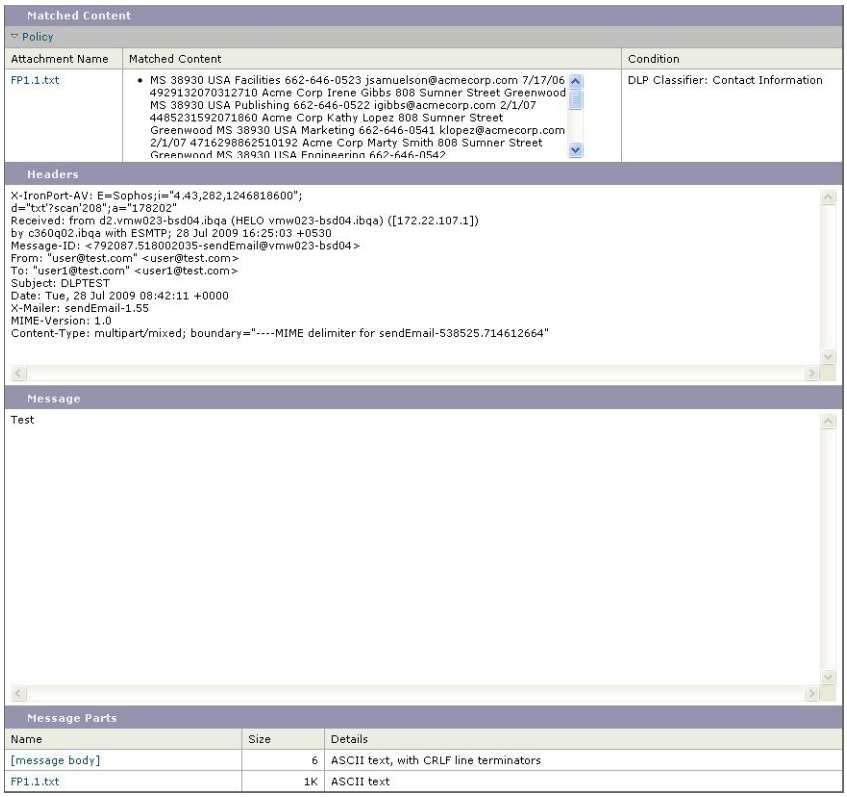
一致した内容の表示

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検疫アクションを設定した場合、検疫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共に表示されます。

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共に）GUI で表示されることがあります。GUI の表示は、該当コンテンツを特定するための目安として使用するもので、該当コンテンツの完全なリストであるとは限りません。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 ルールと共に一覧表示するテーブルは正しく表示されます。

図 *1 : Policy* 検疫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。ウイルスが含まれる可能性がある添付ファイルは、ユーザ自身の自己責任においてダウンロードしてください。[メッセージ部分（Message Parts）] セクション内の [メッセージ本文（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

隔離されたすべてのキューからメッセージが解放されるとき、アプライアンスおよび最初にメッセージを隔離したメールポリシーで有効化されている機能によって、次の再スキャンが発生します。

- ポリシーおよびウイルス隔離から解放されるメッセージはアンチウイルス、高度なマルウェア防御、グレイメール 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解放されたメッセージは、アンチスパム、AMP、およびアンチウイルス エンジンによって再スキャンされます。

- ファイル分析隔離から解放されるメッセージは、脅威に対する再スキャンが実行されます。
- 添付ファイルを含むメッセージは、ポリシー、ウイルス、およびアウトブレイク隔離から解放されるときにファイル レピュテーション サービスによって再スキャンされます。

再スキャン時に、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、そのメッセージは別の隔離に送信される可能性があります。

原理的に、メッセージの検疫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 検疫に送信されるとします。管理者がそのメッセージを解放しても、アンチウイルス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ります。再隔離されるとループ状態となり、そのメッセージは隔離からまったく解放されなくなります。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 検疫を無視します。

アウトブレイク隔離

Outbreak 検疫は、Outbreak 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。Outbreak 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 Outbreak 検疫に送信されます。詳細については、E 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。

アウトブレイク隔離は、他の隔離と同様の機能を持ち、メッセージを検索したり、メッセージを解放または削除したりなどできます。

アウトブレイク隔離には次のビューがあります。

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（[ルールサマリー（Rule Summary）] ビュー、メッセージの詳細を表示しているときの**シスコへの送信**機能、および**スケジュールされた保存期間の終了**日時で検索結果内のメッセージを並べ替えるオプション）。

アウトブレイク 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。

関連項目

- アウトブレイク隔離のメッセージの再スキャン （34 ページ）
- ルール サマリー ビュー （34 ページ）
- シスコへの偽陽性または不審なメッセージの報告 （34 ページ）

アウトブレイク隔離のメッセージの再スキャン

アウトブレイク隔離に入れられたメッセージは、新しく公開されたルールによってもう脅威ではないと見なされると、自動的に解放されます。

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 サマリー ビュー

[ルール サマリ（Rule Summary）] ビューは、新しい Web インターフェイスでのみ利用可能です。

アウトブレーク隔離で、[ルールサマリー（Rule Summary）] タブをクリックして、アウトブレーク隔離のコンテンツのリストをルール ID ごとにグループ化して表示します。

検疫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検疫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（リリースおよび削除）を実行できます。これは、アウトブレイク隔離から多数のメッセージを片付ける場合に適しています。詳細については、*E* メールセキュリティアプライアンス向け *AsyncOS* のオンラインヘルプまたはユーザガイドの「Outbreak Filters」の章の「Outbreak Quarantine and the Manage by Rule Summary View」の項を参照してください。

[ルール サマリー管理（Manage by Rule Summary）] リンク

検疫リストで Outbreak 検疫の横にある [ルール概要による管理（Manage by Rule Summary）] リンクをクリックして、[ルール概要による管理（Manage by Rule Summary）] ページを表示します。検疫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検疫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多数のメッセージを片付ける場合に適しています。詳細については、E 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 [ルールサマリーによる管理（Manage by Rule Summary）] ビューについての情報を参照してください。

シスコへの偽陽性または不審なメッセージの報告

アウトブレイク隔離内のメッセージについてメッセージの詳細を表示しているとき、偽陽性または不審なメッセージを報告するためにそのメッセージをシスコへ送信できます。

ステップ 1 アウトブレイク隔離内のメッセージの移動

ステップ 2 受信者のアドレスを入力し、**[送信（Send）]** をクリックします。

集約されたポリシー隔離のトラブルシューティング

管理ユーザがフィルタおよびDLPメッセージアクションの隔離を選択できない

問題

管理ユーザが、Eメールセキュリティアプライアンスに対するコンテンツフィルタおよびメッセージフィルタまたはDLPアクションの隔離を表示することも選択することもできません。

解決方法

カスタム ユーザ ロールの集約隔離アクセスの設定 （11ページ）を参照してください

集約アウトブレイク隔離から解放されたメッセージが再スキャンされない

問題

アウトブレイク隔離から解放されたメッセージは配信前に再スキャンされるはずですが、一部の汚染されたメッセージが隔離から配信されました。

解決方法

これは、次で説明した状況で発生する可能性があります隔離されたメッセージの再スキャンについて （32ページ）

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。