# 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。


- ポリシー、ウイルス、およびアウトブレイク隔離の概要 （1 ページ）
- 集約隔離の概要 （2 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 （5 ページ）
- 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 （14 ページ）


## ポリシー、ウイルス、およびアウトブレイク隔離の概要

「ポリシー、ウイルス、およびアウトブレイク隔離」には、ファイル分析の隔離を含むすべての非スパム隔離が含まれます。

E メール セキュリティ アプライアンスは危険性のあるマルウェア、または組織で許可されていないコンテンツを送受信メッセージで検出した場合、すぐに削除せずに隔離エリアに送信します。隔離エリアはこれらのコンテンツを E メール セキュリティ アプライアンスまたは Cisco コンテンツ セキュリティ管理アプライアンスで一定期間安全に保持し、ユーザがそれらを評価するまで、またはメッセージの安全性を適切に評価できるアップデートまで待ちます。

組織での非スパム隔離の使用例：

- **ポリシーの実施。**人事担当部門または法務部門が、それらに不快な情報や秘密情報などの許可されない情報が含まれていないか確認します。
- **ウイルス隔離。**ユーザへのウイルスの拡散を防ぐためのアンチウイルス スキャン エンジンによって、暗号化メッセージや感染メッセージまたはスキャン不可能とマークされたメッセージを保管します。
- **アウトブレイクの防止。**アウトブレイク フィルタによってウイルスのアウトブレイクの一部または小規模なマルウェア攻撃としてフラグ付けされたメッセージを、アンチ ウイルスまたはアンチ スパム アップデートがリリースされるまで保管します。
- **ファイル分析の隔離。**判定に到達するまで、分析用に送信されたマルウェアを含む可能性がある添付ファイルを含むメッセージを保存します。

# 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。

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 | 追加情報 |
|---|---|---|---|---|
| 高度なマルウェア対策 | ファイル分析 | ○ | 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。 | |
| 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。<br>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。<br>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」） | なし | 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 | 追加情報 |
|---|---|---|---|---|
| | | | | • ポリシー、ウイルス、およびアウトブレイク隔離の管理（5 ページ）<br>• ポリシー、ウイルス、またはアウトブ |

| 隔離タイプ | 隔離名 | デフォルトで作成される | 説明 | 追加情報 |
|---|---|---|---|---|
| | | | | レイク隔離のメッセージの操作（14ページ） |
| 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。<br>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

ポリシー、ウイルス、およびアウトブレイク隔離のディスク領域の詳細については、ディスク領域の管理 を参照してください。

隔離を集約しても、ポリシー、ウイルス、およびアウトブレイク隔離は、E メール セキュリティ アプライアンスのディスク領域を消費します。

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 E メール セキュリティ 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 E 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、

# 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。メッセージの保持期間は、隔離ごとに指定します。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 （5 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、新しいメッセージの領域を確保するために隔離内にあるメッセージが配信されます。

    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 （12 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 （7 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 （6 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：メッセージを隔離からリリースして配信します。

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 （20 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 （7 ページ）を参照してください。

# 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。

# 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 （9 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 （6 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 （7 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 （13 ページ）を参照してください。

**ステップ 1** [モニタ（Monitor）] > [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** 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 3** 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。
- 隔離ディスクに空き領域がなくなった場合でも、指定した保持期間前にその隔離内のメッセージが処理されなくなるように設定するには、[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）] 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。<br>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。<br>（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。 |
| X-Header の追加（Add X-Header） | X-Header には、メッセージで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。<br>名前と値を入力します。<br>例：<br>Name = Inappropriate-release-early<br>Value = True |

| オプション | 情報 |
|---|---|
| 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 4** この隔離へのアクセスを付与する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。<br>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（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 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 5** 変更を送信し、保存します。

### 次のタスク

メッセージおよびコンテンツ フィルタ、メッセージを隔離エリアに移動する DLP メッセージ アクションを作成します。

# 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 （6 ページ）も参照してください。

隔離の設定を変更するには、[アプライアンス設定（Appliance Configuarion）]ページから [モニタ（Monitor）] > [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）] [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 検証プロファイルを表示できます。

**ステップ 1** [モニタ（Monitor）] > [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** ポリシー隔離の名前をクリックします。

**ステップ 3** 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 （10 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 （7 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。

# 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

| 内容 | 操作手順 |
|---|---|
| スパム隔離以外のすべての隔離に割り当てられている領域の合計を確認する | ページを選択し、その最初のセクションを確認します。<br>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 | **[モニタ（Monitor）] > [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。 |

| 内容 | 操作手順 |
|---|---|
| 現在すべての隔離が使用している合計容量を確認する | [モニタ（Monitor）] > [システム ステータス（System Status）] を選択し、[隔離に使用されるキュー スペース（Queue Space Used by Quarantine）] を探します。<br>[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。 |
| 現在各隔離に使用されている容量を確認する | **[モニタ（Monitor）]>[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 | [モニタ（Monitor）] > [システム ステータス（System Status）] を選択し、[隔離内のアクティブ メッセージ（Active Messages in Quarantine）] を探します。<br>[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 | [モニタ（Monitor）]>[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 | [モニタ（Monitor）] > [システム ステータス（System Status）] を選択し、[CPU 使用率（CPU Utilization）] セクションを確認します。<br>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（ポリシー隔離間の移動を除く）を確認する | [モニタ（Monitor）]>[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<br>ポリシー隔離の作成者の名前を確認する | **[モニタ（Monitor）]>[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。<br>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。 |

| 内容 | 操作手順 |
| --- | --- |
| 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 （10ページ）を参照してください。 |

# ポリシー隔離のパフォーマンス

ポリシー隔離エリアに保存されたメッセージは、ハード ドライブ容量に加えて、システム メモリを使用します。1 つのアプライアンスのポリシー隔離エリア内で数十万メッセージを保存すると、過剰なメモリ使用によりアプライアンスのパフォーマンスが低下することがあります。アプライアンスでのメッセージの隔離、削除、および解放により多くの時間が必要になるため、メッセージ処理の速度が低下し、電子メール パイプラインが渋滞します。

E メール セキュリティ アプライアンスが通常の速度で電子メールを処理できるように、ポリシー隔離には平均で 20,000 よりも少ないメッセージを保存することをお勧めします。

隔離のメッセージ数を調べるには、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 （10 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。

アラートの詳細については、アラート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)

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。

## 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。
- Operators、Guests、Read-Only Operators、および Help Desk Users グループに属するユーザに加え、隔離の管理権限を持つカスタム ユーザ ロールのユーザは、隔離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 リンクおよび、隔離されたメッセージに関する情報が表示されません。

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。

# クラスタ設定におけるポリシー、ウイルス、およびアウトブレイク隔離について

ポリシー、ウイルス、およびアウトブレイク隔離は、中央集中型管理を使用した展開でマシンレベルでのみ設定できます。

# ポリシー、ウイルス、アウトブレイク隔離の設定の集約方法

Cisco コンテンツ セキュリティ管理アプライアンス上でポリシー、ウイルス、およびアウトブレイク隔離を中央集中型にできます。詳細については、次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集約

# 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

## 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 | [モニタ（Monitor）] > [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。<br>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。 |
| アウトブレイク隔離エリアのメッセージを表示する | [モニタ（Monitor）] > [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。<br>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。<br>[ルール サマリー管理（Manage by Rule Summary）] リンク（21 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。 |
| 隔離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）。 |

| 目的 | 操作手順 |
|---|---|
| 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。 |
| 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 （18 ページ）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 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化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索

（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）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 2** **[モニタ（Monitor）] > [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 3** [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 4** （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 （16 ページ）を参照してください。

# 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。

- [モニタ（Monitor）] > [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）]または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。
- [隔離全体を検索（Search Across Quarantines）] をクリックするとき。
- 隔離の名前をクリックし、隔離内を検索するとき。

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。を参照してください。

## 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。
- 複数の隔離内に格納されているメッセージをそのコピーを保持している場所に移動した場合、移動したメッセージの有効期限および隔離理由により、移動先にあるメッセージの情報が上書きされます。

# 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ウイルス検査を実行したりできます。また、メッセージが検疫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。

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 （20 ページ）を参照してください。

## 一致した内容の表示

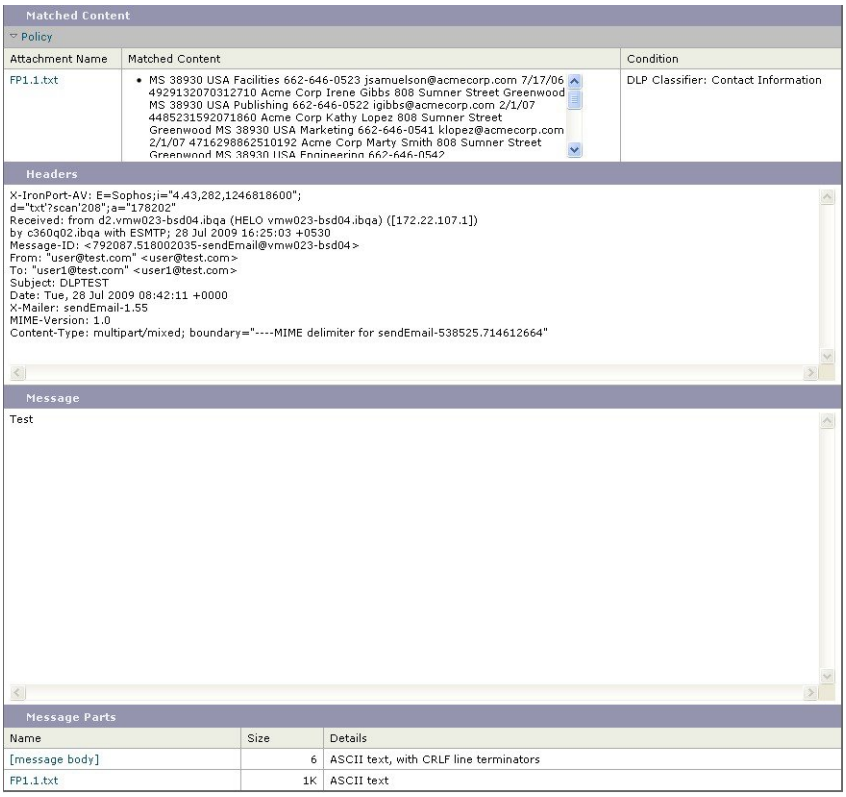
Attachment Content 条件、Message Body または Attachment 条件、Message 本文条件、または Attachment 内容条件と一致するメッセージに対して検疫アクションを設定した場合、検疫されたメッセージ内の一致した内容を表示できます。メッセージ本文を表示する場合、DLP ポリシー違反の一致を除き、一致した内容が黄色で強調表示されます。また、$MatchedContent ア

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。

### ウイルス テスト

メッセージがウイルスに感染していないかどうかを検査するには、[テスト開始（Start Test）]をクリックします。アンチウイルス シグニチャが最新のものであることを確認できるまで、メッセージの保管に隔離を使用します。

ウイルスの検査では、オリジナルのメッセージではなく、メッセージのコピーがアンチウイルス エンジンに送信されます。アンチウイルス エンジンの判定結果は、[隔離（Quarantines）]エリアの上に表示されます。

## 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 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。（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、を参照してください）
- 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、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。

- 標準（Standard）
- ルールのサマリー

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（[ルールサマリーによる管理（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。検疫エリア内に現在存在するメッセージの保持期間が終了して Outbreak 検疫が空になると、GUI の検疫リストに Outbreak 検疫は表示されなくなります。

## 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、Outbreak 検疫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、「[アウトブレイク隔離（Outbreak Quarantine）]および[ルールサマリーによる管理（Manage by Rule Summary）] ビュー」に記載のトピック 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エリア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。