CHAPTER 10

ウイルス感染フィルタ

IronPort のウイルス感染フィルタ機能を使用することで、ウイルスとの格闘において「優位なスタート」を切ることができます。歴史的に、新しいウイルスまたはウイルスの変異形がインターネットを攻撃した場合、最も危機的な期間はウイルスがリリースされてからアンチウイルス ベンダーがアップデートしたウイルス定義をリリースするまでの期間です。たとえ数時間でも、事前に通知を受けることは、悪意のあるコードの拡散を抑えるうえで非常に重要です。その脆弱な期間で、現代のウイルスはグローバルに伝播し、電子メール インフラストラクチャを停止に追い込むことが可能です。

IronPort のウイルス感染フィルタは、積極的にアクションを実行して、新しいアウトブレイクに対する防御において、非常に重要な第 1 のレイヤを提供します。IronPort のウイルス感染フィルタは、リアルタイムで新しいアウトブレイクを検出し、動的に応答して疑いのあるトラフィックのネットワークへの侵入を防ぐことで、新しいアンチウイルス署名のアップデートが展開されるまでの間の保護を提供します。IronPort の電子メール セキュリティ アプライアンスに統合されたウイルス感染フィルタには、アウトブレイク検出テクノロジーと、IronPort に実装されたインテリジェントな検疫システムという 2 つの主要コンポーネントがあります。

IronPort の業界をリードするウイルス感染フィルタ テクノロジーは、いったんイネーブルにした後は管理者の操作を必要としない、「ファイア アンド フォーゲット」機能（標的を自動的に追尾する能力）を提供します。このテクノロジーは、2 つの異なる一連のルールを使用して、高い有効性を持ち、綿密に的を絞った、一連のウイルス検出基準を提供することで、フィルタが確実に特定の脅威に正確に照準を合わせることができるようにしています。ウイルス感染フィルタのルールおよびアクションは、水面下に隠されているものではなく、管理者の目に見えるようになっており、検疫されたメッセージにただちにアクセスしたり、検疫された理由を確認したりできるようになっています。

IronPort アプライアンスには、ウイルス感染フィルタ機能の 30 日評価ライセンスが同梱されています。

この章は、次の内容で構成されています。

ウイルス感染フィルタの概要

ウイルス感染フィルタ エンジンは、着信メッセージと、発行されているウイルス感染フィルタ ルールを比較します。ルールと一致したメッセージには、脅威レベルが割り当てられ、さらにその脅威レベルは、お客様が設定した脅威レベルのしきい値と比較されます。しきい値以上のメッセージは、検疫されます。

アウトブレイクの検出およびフィルタリングの処理は、SenderBase から開始されます。SenderBase は、2 千万を超える IP アドレスを追跡し、世界の電子メール トラフィックの約 25 % を把握しています。IronPort は、SenderBase の履歴データを使用して、正常なグローバル トラフィック パターンの統計的なビューを作成します。ウイルス感染フィルタ エンジンは、着信メッセージの脅威レベルの決定に使用される一連のルールに依存しています。

ウイルス感染フィルタ：次世代の予防的ソリューション

ウイルス感染フィルタ機能は、機能およびユーザビリティが大幅に拡張されています。大まかには、この拡張には次の内容が含まれます（ただし、これに限定されるものではありません）。

- 粒度を増したアウトブレイク ルール（アンチウイルス署名ルールを含む）
- Context Adaptive Scanning Engine（CASE）スキャンの追加
- アダプティブ ルールの追加
- 動的検疫（定期的なメッセージの再評価、アンチウイルス アップデートに基づく自動解除、拡張オーバーフロー オプションなど）
- 検疫管理の向上（拡張された可視性、検索またはソート オプション、アラートなど）

これらの機能拡張は、システムによるアウトブレイクの捕捉率を向上し、アウトブレイクの可視化を強化するとともに、使いやすさや、アウトブレイク メッセージの管理しやすさを向上することを目的としています。

ルールのタイプ：アダプティブ ルールおよびアウトブレイク ルール

バージョン 4.5 よりも前のバージョンでは、ウイルス アウトブレイク ルールは添付ファイル タイプのみに基づいており、そうしたルールとして、ただ 1 つのルール タイプ（添付ファイル タイプに縛られているもの）が使用されていました。AsyncOS バージョン 4.5 からは、ウイルス感染フィルタでは「アダプティブ」および「アウトブレイク」という 2 つのタイプのルールが使用されます。

アウトブレイク ルール

アウトブレイク ルールは、IronPort Threat Operations Center（TOC）で作成されるもので、添付ファイルのタイプだけでなく、メッセージ全体に焦点を当てています。アウトブレイク ルールは、SenderBase データ（リアルタイムおよび履歴のトラフィック データ）およびその他のあらゆるメッセージ パラメータの組み合わせ（添付ファイル タイプ、ファイル名のキーワード、またはアンチウイルス エンジンのアップデート）を使用して、リアルタイムでウイルスのアウトブレイクを認識し、防止します。アウトブレイク ルールには一意の ID が付けられ、GUI のさまざまな場所（たとえば Outbreak 検疫など）でルールを参照するために使用されます。

グローバル SenderBase ネットワークからのリアルタイム データは、このベースラインと比較され、アウトブレイクの確かな前兆である異常を識別します。IronPort Threat Operations Center（TOC）は、データをレビューして脅威のインジケータまたは Virus Threat Level（VTL）を発行します。VTL は、メッセージにウイルスが含まれており、かつそのウイルスに対するその他のゲートウェイ防御が IronPort の顧客には広く展開されていない可能性を計測して、0（脅威なし）～ 5（きわめて危険）の数値で表すものです（詳細については、「Virus Threat Level（VTL）」（P.10-341）を参照してください）。VTL は、TOC によりアウトブレイク ルールとして発行されます。

アウトブレイク ルール内で組み合わせることができる特性には、たとえば次のようなものがあります。

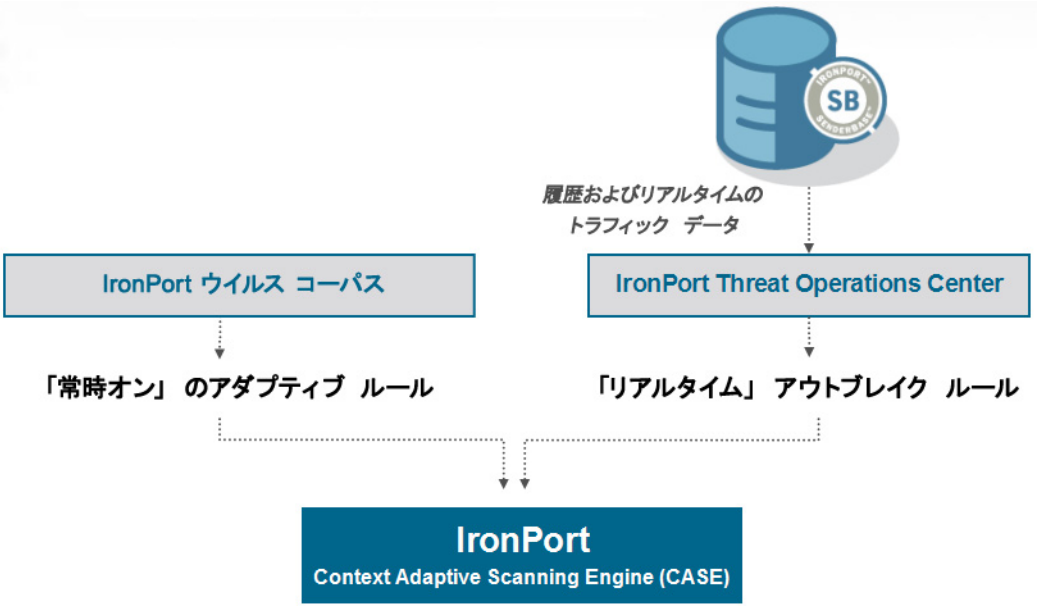
- ファイル タイプ、ファイル タイプとサイズ、ファイル タイプとファイル名キーワードなど

- ファイル名キーワードとファイル サイズ
- ファイル名キーワード
- メッセージ URL
- ファイル名と Sophos IDE

アダプティブ ルール

アダプティブ ルールは、CASE 内の一連のルールであり、対象のメッセージの属性と、既知のウイルス性メッセージおよびアウトブレイク メッセージの属性を正確に比較します。これらのルールは、IronPort の広範なウイルス コーパスの中で、既知のウイルス性メッセージおよび既知の良好なメッセージを研究し、作成されたものです。アダプティブ ルールは、コーパスの評価に合わせて、頻繁にアップデートされます。アダプティブ ルールは、既存のアウトブレイク ルールを補完して、常にアウトブレイク メッセージを検出します。アウトブレイク ルールは、アウトブレイクの可能性がある状態が発生したときに有効になりますが、アダプティブ ルールは（いったんイネーブルにされると）「常時オン」となり、グローバルな規模で本格的な異常が起きる前にローカルでアウトブレイク メッセージを捕捉します。さらに、アダプティブ ルールは、電子メール トラフィックおよび構造の小規模および微小な変化にも継続的に対応し、お客様にアップデートした保護を提供します。

図 10-1　検出：複数の方法と多くのパラメータ



アウトブレイク

ウイルス感染フィルタ ルールは、基本的に VTL（例：4）で、電子メールのメッセージおよび添付ファイルの一連の特性（ファイル サイズ、ファイル タイプ、ファイル名、メッセージの内容など）に関連付けられています。たとえば、ファイル名に特定のキーワード（たとえば「hello」）が含まれた .exe 形式のファイル（サイズは 143 KB）が添付された、疑わしい電子メール メッセージの発生が増加していることを、IronPort TOC が通知したと想定します。この基準に一致するメッセージに対する VTL を増加したアウトブレイク ルールが発行されます。デフォルトでは、IronPort アプライアンスは、新しく発行されたアウトブレイクおよびアダプティブ ルールを 5 分ごとにチェックし、ダウンロードします（「ウイルス感染フィルタ ルールのアップデート」（P.10-351）を参照）。アダプティブ ルールは、それほど頻繁にはアップデートされません。IronPort アプライアンスで、検疫のしきい値を設定します（例：3）。メッセージの VTL がこのしきい値以上の場合、メッセージは *Outbreak* 検疫エリアに送信されます。

検疫およびアンチウイルス スキャン

これらのメッセージを検疫することで、アップデートされたアンチウイルス定義が作成され、インストールされるまでの期間、検疫エリアがバッファの役割を果たします。この間隔は、ウイルスへの接触および企業内でのウイルスの蔓延を制限するうえで、きわめて重要です。メッセージは、Outbreak 検疫エリアから解放された時点で、再度アンチウイルス スキャンにかけられます。また、アプライアンスがアンチスパム フィルタを使用している場合は、メッセージは検疫エリアから解放された時点で、再度アンチスパム スキャンにもかけられます。詳細については、「動的検疫」（P.10-344）を参照してください。

次の手順には、検疫されたメッセージ自体の処理が含まれます。メッセージを検疫しておく予定時間の長さ、およびメッセージの検疫が解除されたときに実行されるアクションは、[Quarantines] ページで設定できます。検疫の全般的な使用方法に関する詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。ウイルス感染フィルタおよび Outbreak 検疫の併用に関する詳細については、「ウイルス感染フィルタ機能および Outbreak 検疫」（P.10-354）を参照してください。

（注） ウイルス感染フィルタ機能は、IronPort アプライアンスでアンチウイルス スキャンをイネーブルにしなくても使用できます。この 2 つのセキュリティ サービスは、お互いを補完するように設計されていますが、別々に動作しています。ただし、IronPort アプライアンスでアンチウイルス スキャンをイネーブルにしていない場合は、アンチウイルス ベンダーのアップデートをモニタリングして、Outbreak 検疫エリアにあるメッセージの一部を手動で検疫解除したり、再評価したりする必要があります。アンチウイルス スキャンをイネーブルにしないでウイルス感染フィルタを使用する場合は、次の点に注意してください。

- アダプティブ ルールはディセーブルにする必要があります。
- メッセージはアウトブレイク ルールに従って検疫されます。
- 脅威レベルが引き下げられたり、検疫時間の期限が過ぎたりした場合は、メッセージは検疫解除されます。
- ダウンストリームのアンチウイルス ベンダー（デスクトップおよびグループウェア）は、検疫解除されたメッセージを捕捉する場合があります。

Virus Threat Level（VTL）

表 10-1（P.10-341）に、各レベルの基本的なガイドラインまたは定義のセットを示します。

表 10-1　Virus Threat Level の定義

VTL	リスク	意味
0	なし	新しいウイルス脅威の既知のリスクはありません。
1	低	非常に小規模のウイルス脅威の疑いがあります。
2	低または中	小～中規模のウイルス脅威の疑いがあります。
3	中	確認されている脅威、または中～大規模の疑いのある脅威があります。
4	高	大規模または非常に危険な、確認されている脅威があります。
5	きわめて高	きわめて大規模、または大規模かつきわめて危険な、確認されている脅威があります。

各アウトブレイク ルールおよび関連する VTL は、次の URL で入手できます。

`http://support.ironport.com/outbreaks/`

このサイトには、現在のアウトブレイク ルールのリストが示されており、IronPort Threat Operations Center（TOC）による各ルールに関するコメントも含まれています。アウトブレイクのレポート方法については、このサイトを参照してください。

アウトブレイク ルールの [View] リンクをクリックすると、特定の拡張子タイプに関連する、すべてのアウトブレイク ルールの履歴を表示できます。

（注） このサイトは、パスワードで保護されています。サイトにアクセスできない場合は、IronPort カスタマー サポートにお問い合わせください。

VTL およびアウトブレイク ルールの詳細については、「ウイルス感染フィルタ ルール」（P.10-350）を参照してください。

脅威レベルのしきい値設定ガイドライン

脅威レベルのしきい値を使用することで、管理者は疑いのあるメッセージをより積極的または消極的に検疫できるようになります。低い値（1 または 2）は、より積極的な設定値で、多くのメッセージが検疫されます。反対に、高いスコア（4 または 5）は消極的な設定値で、ウイルスに感染している可能性がきわめて高いメッセージのみが検疫されます。

IronPort は、デフォルト値の 3 を推奨します。

ウイルス感染フィルタの機能概要

電子メール メッセージは、IronPort アプライアンスで処理される際に、「電子メール パイプライン」と呼ばれる一連の手順を通過します（電子メール パイプラインの詳細については、「電子メール パイプラインの理解」（P.4-91）を参照してください）。メッセージは、電子メール パイプラインを通過しながら、Anti-Spam（AS; アンチスパム）および Anti-Virus（AV; アンチウイルス）スキャン エンジンにかけられます（対象のメール ポリシー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のみ）。これらのスキャンを通過するメッセージのみ、ウイルス感染フィルタ機能によりスキャンされます（ウイルス感染フィルタ機能によりスキャンされるメッセージの決定に電子メール パイプラインがどのように影響を及ぼすかについての詳細は、「メッセージ フィルタ、コンテンツ フィルタ、および電子メール パイプライン」（P.10-360）を参照してください）。言い換えると、認識されているウイルスが含まれる既知のスパムまたはメッセージは、ウイルス感染フィルタ機能でスキャンされる前に、アンチスパムおよびアンチウイルス設定に基づいてメール ストリームから除去（削除、検疫など）されているため、ウイルス感染フィルタ機能ではスキャンされません。このため、ウイルス感染フィルタ機能に到達するメッセージは、ウイルスに感染していないとマークされています。

メッセージ スコアリング

新しいウイルスがコンピュータ ネットワークに放たれた時点では、それがウイルスであると認識できるアンチウイルス ソフトウェアはまだありません。ウイルス感染フィルタ機能が非常に重要となるのは、このときです。着信メッセージは、CASE によりスキャンおよびスコアリング（つまり、各メッセージが発行されているアウトブレイクおよびアダプティブ ルールと比較）されます（「ルールのタイプ：アダプティブ ルールおよびアウトブレイク ルール」（P.10-337）を参照）。メッセージに該当するルールがあった場合は、どのルールに一致したかに

従って、対応する Virus Threat Level（VTL）が割り当てられます。メッセージに複数のスコア（アウトブレイクおよびアダプティブ ルールによるもの）が割り当てられた場合については、「メッセージ スコアリング、Context Adaptive Scanning Engine、およびウイルス感染フィルタ」（P.10-343）を参照してください。関連する VTL が存在しない（メッセージに一致するルールが存在しない）場合は、メッセージにはデフォルトの VTL である 0 が割り当てられます。

その計算が完了すると、ウイルス感染フィルタ機能は、メッセージの VTL が設定したしきい値以上であるかどうかをチェックします。しきい値以上である場合は、メッセージは検疫されます。しきい値未満の場合は、パイプラインの後続の処理が継続されます。

メッセージ スコアリング、Context Adaptive Scanning Engine、およびウイルス感染フィルタ

ウイルス感染フィルタには、IronPort 独自の Context Adaptive Scanning Engine（CASE）が使用されています。CASE は、メッセージング脅威に対するリアルタイムの分析に基づいて自動的かつ定期的に調整されている、100,000 を超える適応メッセージ属性を活用しています。ウイルス感染フィルタの場合、CASE はメッセージの内容、コンテキスト、および構造を分析してアダプティブ ルールのトリガーである可能性のあるものを、正確に識別します。

CASE は、アダプティブ ルールと Threat Operations Center（TOC）から発行されるリアルタイムのアウトブレイク ルールを組み合わせて、各メッセージにスコアを付け、独自の Virus Threat Level（VTL）を割り当てます。この VTL は、アプライアンスにプリセットされた検疫しきい値と比較され、しきい値のレベル以上の場合は、自動的にメッセージの検疫が開始されます。

さらに、CASE は既存の検疫されているメッセージを発行されている最新のルールに照らして再評価し、メッセージの最新の脅威レベルを決定します。これにより、アウトブレイク メッセージに整合する脅威レベルを持つメッセージのみが検疫され続け、脅威と見なされなくなったメッセージは自動再評価の後に検疫エリアから解放されます。

CASE の詳細については、「IronPort Anti-Spam および CASE の概要」（P.8-264）を参照してください。

複数のスコアが存在する場合（1 つのスコアが、あるアダプティブ ルールに基づいたもの（または該当するアダプティブ ルールが複数ある場合はそのうちの最も高いスコア）で、別のスコアはあるアウトブレイク ルールに基づいたもの

（または該当するアウトブレイク ルールが複数ある場合はそのうちの最も高いスコア）である場合）は、インテリジェント アルゴリズムを使用してスコアが決定されます。

動的検疫

ウイルス感染フィルタ機能の Outbreak 検疫エリアは、新しいウイルス定義が作成されて、アンチウイルス ソフトウェアがアップデートされるまでの間、一時的にメッセージを保管しておくための保持領域です。詳細については、「アウトブレイク ライフサイクルおよびルール発行」（P.10-345）を参照してください。検疫されたメッセージは、複数の方法で Outbreak 検疫エリアから解放されます。新しいアウトブレイク ルールがダウンロードされると、Outbreak 検疫エリアにあるメッセージは、最も長く検疫されているメッセージから自動的に再評価されます。更新されたメッセージの脅威レベルがシステムのしきい値よりも低くなった場合、メッセージは自動的に（Outbreak 検疫の設定に関係なく）検疫解除されるため、メッセージが検疫されている時間を最小限に抑えることができます。メッセージの再評価中に新しいルールが発行された場合は、再スキャンが開始されます。

新しいアンチウイルス署名が使用可能な場合は、メッセージが自動的に Outbreak 検疫エリアから解放されることはないため、注意してください。発行された新しいルールは、新しいアンチウイルス署名を参照している場合と、参照していない場合があります。ただし、メッセージは、アウトブレイク ルールによりメッセージの脅威レベルが設定されている脅威レベルのしきい値よりも低いスコアに変更されない限り、アンチウイルス エンジンがアップデートされたことによって検疫解除されることはありません。

また、タイムアウト時間（デフォルトは 24 時間）を経過した場合も、メッセージは Outbreak 検疫エリアから解放されます。メッセージは、手動で検疫解除できます。また、検疫エリアがいっぱいであるときに、追加のメッセージが挿入されると、メッセージが検疫解除される場合があります（これはオーバーフローと呼ばれます）。オーバーフローは、Outbreak 検疫エリアが容量の 100 % まで使用されているときに、新しいメッセージが検疫エリアに追加された場合のみ発生します。このとき、メッセージが検疫解除される優先順位は次のとおりです。

- アダプティブ ルールにより検疫されたメッセージ（最も早く検疫解除されるようにスケジュール設定されているものから）
- アウトブレイク ルールにより検疫されたメッセージ（最も早く検疫解除されるようにスケジュール設定されているものから）

Outbreak 検疫エリアの使用量が容量の 100 % を下回った時点で、オーバーフローは停止します。検疫エリアのオーバーフローの処理方法に関する詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。

Outbreak 検疫エリアから解放されたメッセージは、再度アンチウイルス フィルタにかけられます。このときに既知のウイルスとしてマークされた場合は、このメッセージはアンチウイルスの設定に従って処理されます（別の検疫エリアである Virus 検疫エリアに検疫される場合もあります）。詳細については、「ウイルス感染フィルタ機能および Outbreak 検疫」（P.10-354）を参照してください。

このため、メッセージのライフタイムの間に、メッセージは 2 回検疫される場合がある（1 回はウイルス感染フィルタ機能により、もう 1 回は Outbreak 検疫エリアから解放されたとき）と注意しておくことが重要です。各アンチウイルス スキャン（ウイルス感染フィルタの前および Outbreak 検疫エリアから解放されたとき）照合の結果、アンチウイルスにより何らかの判断がなされたメッセージは、2 回検疫されることはありません。また、ウイルス感染フィルタ機能により、メッセージに対して最終的なアクションが実行されることはないことにも注意してください。ウイルス感染フィルタ機能は、（後続のアンチウイルス処理を実行するために）メッセージを検疫するか、またはメッセージをパイプラインの次の手順に移動します。

アプライアンスで IronPort Anti-Spam または IronPort Intelligent Multi-Scan を使用している場合は、Outbreak 検疫エリアから解放されたメッセージは、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、アンチスパム フィルタにもかけられます。メッセージがスパムである、スパムの疑いがある、またはマーケティングであると検出された場合は、そのメッセージはアンチスパムの設定に従って処理されます（IronPort スパム検疫で検疫される場合もあります）。アンチスパム フィルタリングの動作概要の詳細については、第 8 章「アンチスパム」を参照してください。

アウトブレイク ライフサイクルおよびルール発行

ウイルスのアウトブレイク ライフサイクルの非常に初期の段階では、メッセージを検疫するために広範なルールが多く使用されます。より詳しい情報が判明していくと、より的を絞ったルールが発行され、検疫する対象の定義が絞り込まれていきます。新しいルールが発行されると、その時点でウイルス メッセージの

可能性があると見なされなくなったメッセージは、検疫解除されます（Outbreak 検疫エリアにあるメッセージは、新しいルールが発行されると再スキャンされます）。

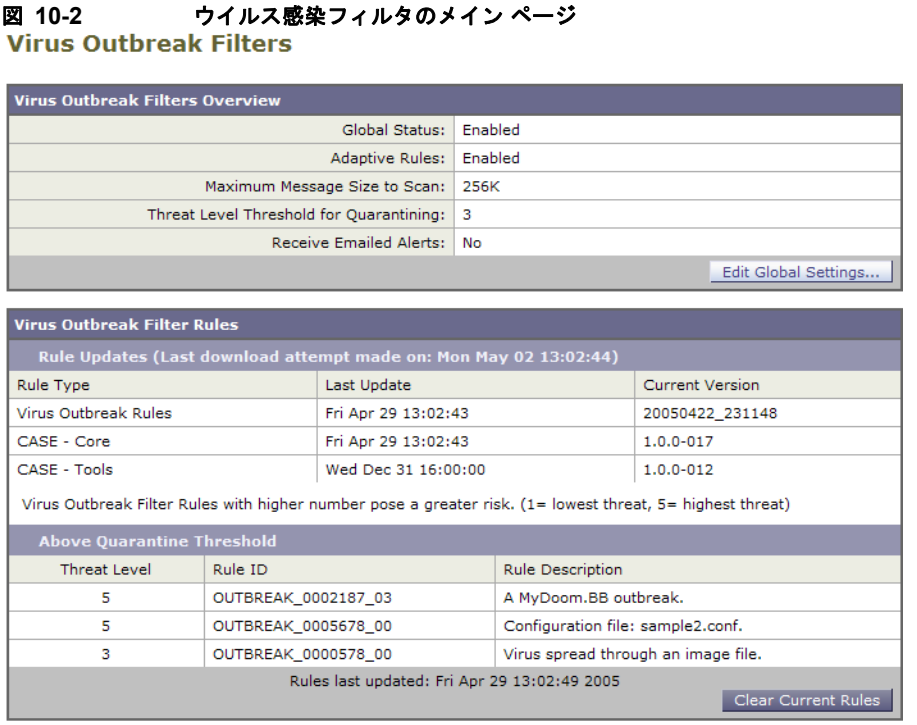
表 10-2　アウトブレイク ライフサイクルのルールの例

時間	ルールの種類	ルールの説明	アクション
T=0	アダプティブ ルール（過去のアウトブレイクに基づく）	10 万を超えるメッセージ属性に基づく、統合されたルールセットで、メッセージの内容、コンテキスト、および構造を分析します。	アダプティブ ルールに一致したメッセージは、自動的に検疫されます。
T=5 分	アウトブレイク ルール	.zip（exe）ファイルが含まれるメッセージを検疫します。	.exe が含まれる .zip 形式の添付ファイルはすべて検疫されます。
T=10 分	アウトブレイク ルール	50 KB を超える .zip（exe）ファイルが含まれるメッセージを検疫します。	50 KB 未満の .zip（exe）ファイルが含まれたメッセージはすべて検疫解除されます。
T=20 分	アウトブレイク ルール	ファイル名に「Price」が含まれる 50 ～ 55 KB の .zip（exe）ファイルが含まれるメッセージを検疫します。	この基準に一致しないメッセージはすべて検疫解除されます。
T=12 時間	アウトブレイク ルール	新しい署名を使用してスキャンします。	残っているすべてのメッセージを、最新のアンチウイルス署名を使用してスキャンします。

ウイルス感染フィルタの管理（GUI）

Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）にログインして [Security Services] タブをクリックします。GUI へのアクセス方法の詳細については、「GUI へのアクセス」（P.2-19）を参照してください。左側のメニューで [Virus Outbreak Filters] リンクをクリックします。

図 10-2　ウイルス感染フィルタのメイン ページ



[Virus Outbreak Filters] ページには、[Virus Outbreak Filters Overview] と現在の [Virus Outbreak Filter Rules]（存在する場合）のリストの 2 つのセクションが表示されます。

図 10-2 の例では、ウイルス感染フィルタはイネーブル、Adaptive Scanning はイネーブル、最大メッセージ サイズは 256 k、脅威レベルのしきい値は 3 に設定されています。これらの設定を変更するには、[Edit Global Settings] をクリックします。グローバル設定の編集に関する詳細については、「ウイルス感染フィルタのグローバル設定の構成」（P.10-348）を参照してください。

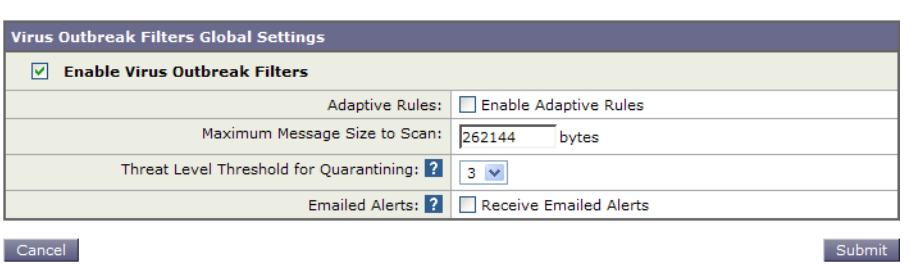
[Virus Outbreak Filter Rules] セクションには、各種コンポーネント（ルール自体だけでなくルール エンジンも含む）の最新アップデートの時刻、日付、およびバージョンのリストと、脅威レベルのしきい値よりも高いまたは低いでソートされた、現在のウイルス感染フィルタ ルールのリストが示されます。

アウトブレイク ルールの詳細については、「ウイルス感染フィルタ ルール」（P.10-350）を参照してください。

ウイルス感染フィルタのグローバル設定の構成

ウイルス感染フィルタのグローバル設定を構成するには、[Edit Global Settings] をクリックします。[Virus Outbreak Filters Global Settings] ページが表示されます。

図 10-3　[Virus Outbreak Filters Global Settings] ページ



このページを使用して、ウイルス感染フィルタをグローバルにイネーブルにしたり、Adaptive Scanning をイネーブルにしたり、スキャンするファイルの最大サイズを設定したり（サイズはバイトで入力します）脅威レベルのしきい値を選択したり、ウイルス感染フィルタのアラートをイネーブルにするかどうかを選択したりします。アラートおよびアダプティブ ルールはデフォルトではイネーブルになっていないため、注意してください。この機能は、`vofconfig` CLI コマンドから使用することもできます（『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照）。設定を変更したら、[Submit] をクリックし、[Commit Changes] をクリックし、必要に応じてオプションのコメントを追加してから、[Commit Changes] をクリックして変更を保存します。

ウイルス感染フィルタ機能のイネーブル化

ウイルス感染フィルタ機能をイネーブルにするには、[Virus Outbreak Filters Global Settings] ページの [Enable Virus Outbreak Filters] の横にあるボックスをオンにして、[Submit] をクリックします。事前にウイルス感染フィルタおよび SenderBase のライセンス契約書に同意しておく必要があります。

いったんグローバルにイネーブルにした後は、ウイルス感染フィルタ機能は、各メール ポリシー（デフォルト ポリシーも含む）に対して個別にイネーブルまたはディセーブルにできます。詳細については、「ウイルス感染フィルタ機能とメール ポリシー」（P.10-352）を参照してください。

ウイルス感染フィルタ機能は、IronPort Anti-Spam スキャンがイネーブルになっているかどうかに関係なく、Context Adaptive Scanning Engine（CASE）を使用します。

ウイルス感染フィルタ機能の詳細については、「電子メール パイプラインとセキュリティ サービス」（P.4-99）を参照してください。

（注）　システムのセットアップ中にライセンスに同意しなかった場合（「手順 4：[Security]」（P.3-62）を参照）は、[Security Services] > [Virus Outbreak Filters] ページで [Enable] をクリックして、ライセンス契約を読み、同意する必要があります。

アダプティブ ルールのイネーブル化

Adaptive Scanning は、ウイルス感染フィルタのアダプティブ ルールをイネーブルにします。メッセージに関する署名情報が使用できない場合は、一連の係数または特性（ファイル サイズなど）が使用されて、メッセージがウイルス性である可能性が決定されます。Adaptive Scanning をイネーブルにするには、[Virus Outbreak Filters Global Settings] ページの [Enable Adaptive Rules] の横にあるボックスをオンにして、[Submit] をクリックします。

脅威レベルのしきい値の設定

リストから脅威レベルのしきい値を選択します。数字が小さいほど検疫されるメッセージは多くなり、数字が大きいほど検疫されるメッセージは少なくなります。IronPort は、デフォルト値の 3 を推奨します。

詳細については、「脅威レベルのしきい値設定ガイドライン」（P.10-342）を参照してください。

ウイルス感染フィルタのアラートのイネーブル化

[Emailed Alerts] というラベルの付いたボックスをオンにして、ウイルス感染フィルタ機能のアラートをイネーブルにします。ウイルス感染フィルタの電子メール アラートのイネーブル化は、単にアラート エンジンをイネーブルにして、ウイルス感染フィルタに関するアラートが送信されるようにするためのものです。送信されるアラートおよび送信先の電子メール アドレスの指定は、[Alerts] ページの [System Administration] タブで設定します。ウイルス感染フィルタのアラートの設定に関する詳細については、「アラート、SNMP トラップ、および

ウイルス感染フィルタ」（P.10-358）を参照してください。

ウイルス感染フィルタ ルール

アウトブレイク ルールは、IronPort Threat Operations Center から発行されます。IronPort アプライアンスは新しいアウトブレイク ルールを 5 分ごとにチェックおよびダウンロードします。

[Virus Outbreak Filters] ページの [Virus Outbreak Filter Status] セクションには、現在のアウトブレイク ルールのリストが、2 つのグループ（[Above Quarantine Threshold] および [Below Quarantine Threshold]）に分けて表示されます。

図 10-4　ウイルス感染フィルタ ルールのリスト

Virus Outbreak Filter Rules

Rule Updates (Last download attempt made on: Wed May 04 12:52:27)

Rule Type	Last Update	Current Version
Virus Outbreak Rules	Tue May 03 11:17:42	20050422_231148
CASE - Core	Wed Dec 31 16:00:00	1.0.0-017
CASE - Tools	Tue May 03 13:33:30	1.0.0-013

Virus Outbreak Filter Rules with higher number pose a greater risk. (1= lowest threat, 5= highest threat)

Above Quarantine Threshold

Threat Level	Rule ID	Rule Description
5	OUTBREAK_0002187_03	A MyDoom.BB outbreak.
5	OUTBREAK_0005678_00	This configuration file was generated by sample2.conf.

Below Quarantine Threshold

Threat Level	Rule ID	Rule Description
3	OUTBREAK_0000578_00	This virus is spread through image files.

Rules last updated: Tue May 3 11:17:46 2005

Clear Current Rules

感染フィルタ ルールの管理

アウトブレイク ルールは自動的にダウンロードされるため、ユーザによる管理は一切必要ありません。

ただし、何らかの理由で IronPort アプライアンスが一定期間 SenderBase の新しいルールにアクセスできない場合は、ローカルでキャッシュされているスコアが有効でなくなっている（つまり、既知のウイルス性の添付ファイル タイプが現

在ではアンチウイルス ソフトウェアのアップデートに含まれている、またはすでに脅威ではなくなっている、またはその両方の場合）可能性があります。この場合は、これらの特性を持つメッセージを検疫しておく必要はありません。

現在のアウトブレイク ルールは、[Clear Current Rules] をクリックして削除できます（CLI で `vofflush` コマンドを発行することと同じです。『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください）。

（注）　GUI で [Clear Current Rules] をクリックした場合、または同じ効果を生じるために CLI で `vofflush` コマンドを使用した場合は、原則的に、IronPort アプライアンスが次に SenderBase から一連の新しいスコアをダウンロードできるようになるまで、*アウトブレイク ルールをディセーブルにしておく*ことになります。アダプティブ ルールはクリアされません。

ウイルス感染フィルタ ルールのアップデート

デフォルトでは、IronPort アプライアンスは 5 分ごとに新しいアウトブレイク ルールのダウンロードを試行します。この間隔は、[Security Services] > [Service Updates] ページで変更できます。詳細については、「システム時刻」（P.15-541）を参照してください。

コンテナ：特定ルールおよび常時ルール

コンテナ ファイルとは、他のファイルを含むジップ（.zip）アーカイブなどのファイルです。TOC は、アーカイブ ファイル内の特定のファイルを処理するルールを発行できます。

たとえば、IronPort TOC により、あるウイルス アウトブレイクが、1 つの .exe が含まれた 1 つの .zip ファイルで構成されていると判別された場合は、.zip ファイル内の .exe ファイル（.zip(exe)）には脅威レベルを設定し、かつ .zip ファイル内に含まれるのその他のファイル タイプ（たとえば .txt ファイル）には特定の脅威レベルを設定しない、特定のアウトブレイク ルールが発行されます。2 番めのルール（.zip(*)）は、コンテナ ファイル タイプ内のその他すべてのファイル タイプをカバーします。コンテナに対する常時ルールは、コンテナ内にある

ファイルのタイプに関係なく、メッセージの VTL 計算に常に使用されます。そのようなコンテナ タイプが危険であると判明した場合は、常時ルールが TOC により発行されます。

表 10-3　フォールバック ルールおよび脅威レベル スコア

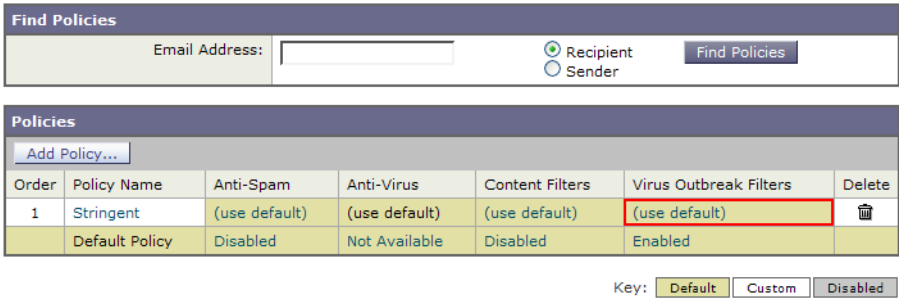
アウトブレイク ルール	脅威レベル	説明
.zip(exe)	4	このルールは、.zip ファイル内の .exe ファイルの脅威レベルを 4 に設定します。
.zip(doc)	0	このルールは、.zip ファイル内の .doc ファイルの脅威レベルを 0 に設定します。
zip(*)	2	このルールは、含まれているファイルのタイプに関係なく、すべての .zip ファイルの脅威レベルを 2 に設定します。

この例では、.zip ファイルに含まれる .foo ファイルの脅威レベルは 2 と見なされます。

ウイルス感染フィルタ機能とメール ポリシー

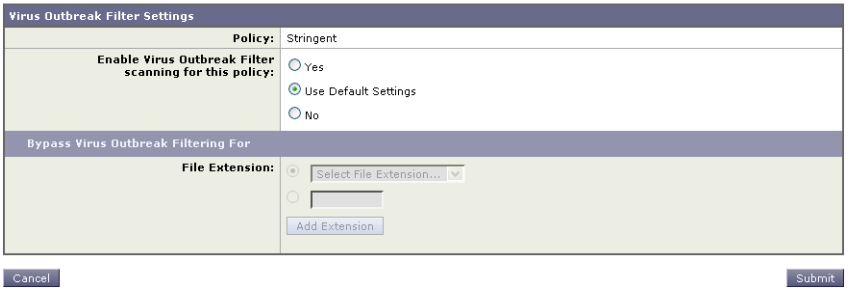
ウイルス感染フィルタ機能の設定には、メール ポリシーごとに設定できるものがあります。ウイルス感染フィルタ機能は、メール ポリシーごとにイネーブルまたはディセーブルにできます。メール ポリシーごとに、特定のファイル拡張子をウイルス感染フィルタ機能の処理から除外できます。この機能は、`policyconfig` CLI コマンドからも使用できます（『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照）。

図 10-5　メール ポリシーのリスト



特定のリスナーに対するウイルス感染フィルタ機能の設定を変更するには、変更するポリシーの [Virus Outbreak Filters] 列のリンクをクリックします。[Virus Outbreak Filter Settings] ページが表示されます。

図 10-6　ウイルス感染フィルタ設定とメール ポリシー



特定のメール ポリシーに対してウイルス感染フィルタ機能をイネーブルにするには、[Yes] を選択します。デフォルト メール ポリシーに対してウイルス感染フィルタ設定を使用するには、[Use Default Settings] を選択します。デフォルト メール ポリシーでウイルス感染フィルタ機能をイネーブルにしている場合は、デフォルトを使用するその他すべてのメール ポリシーでもウイルス感染フィルタ機能がイネーブルになります。設定を変更したら、変更を確定します。

ファイル拡張子タイプのバイパス

特定のファイル タイプをバイパスするようにポリシーを変更できます。バイパスされたファイル拡張子は、CASE エンジンによるメッセージのスコアの計算から除外されます。ただし、添付ファイルに対する残りの電子メール セキュリティ ワークフローの処理は行われます。

ファイル拡張子をバイパスするには、次の手順を実行します。

[Virus Outbreak Filter Settings] ページの [Incoming Mail Policies] で、ファイルの拡張子を選択または入力して、[Add Extension] をクリックします。詳細については、「電子メール セキュリティ マネージャ」（P.6-189）を参照してください。

バイパスされる拡張子のリストから拡張子を削除するには、拡張子の横にあるゴミ箱アイコンをクリックします。

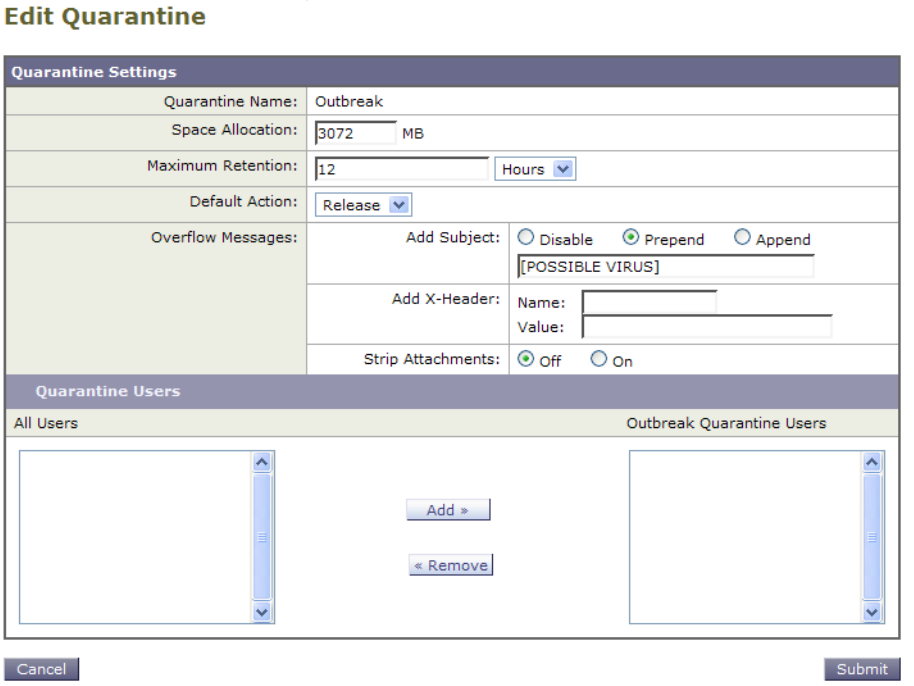
ファイル拡張子のバイパス：コンテナ ファイルのタイプ

ファイル拡張子をバイパスする場合、コンテナ ファイル内のファイル（たとえば .zip 内の .doc ファイル）もバイパスする拡張子のリストに含まれていれば、バイパスされます。たとえば、バイパスする拡張子のリストに .doc を追加した場合は、コンテナ ファイルに含まれているものも含めて、すべての .doc ファイルがバイパスされます。

ウイルス感染フィルタ機能および Outbreak 検疫

ウイルス感染フィルタ機能により検疫されたメッセージは、Outbreak 検疫エリアに送信されます。この検疫エリアは、メッセージを検疫するために使用されるルール（アウトブレイク ルールの場合はアウトブレイク ID、アダプティブ ルールの場合は一般名称が表示されます）に基づいて、検疫エリアからすべてのメッセージを削除または解放する際に役立つ「サマリー」ビューがあることを除けば、その他のあらゆる検疫と同様に機能します（検疫の操作方法の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください）。サマリー ビューの詳細については、「[Outbreak Quarantine] および [Manage by Rule Summary] ビュー」（P.10-357）を参照してください。

図 10-7　Outbreak 検疫



Outbreak 検疫のモニタリング

適切に設定された検疫エリアはほとんどモニタリングを必要としませんが、特にウイルス アウトブレイクの発生中または発生後の、正規のメッセージが遅延する可能性がある間は、Outbreak 検疫エリアに注意を払うことを推奨します。

正規のメッセージが検疫された場合、Outbreak 検疫の設定によっては、次のようになります。

- 検疫のデフォルト アクションが解放に設定されている場合は、保持時間の期限が切れたとき、または検疫エリアがオーバーフローしたときにメッセージが解放されます。オーバーフローのためにメッセージが解放される前に、添付ファイルの削除、件名の変更、X-Header の追加といったアクションがメッセージに対して実行されるように、Outbreak 検疫を設定できます。これらのアクションの詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。

- 検疫のデフォルト アクションが削除に設定されている場合は、保持時間の期限が切れたとき、または検疫エリアがオーバーフローしたときにメッセージが削除されます。
- オーバーフローは、検疫エリアがいっぱいのときにさらにメッセージが追加された場合に発生します。この場合は、有効期限日に近いメッセージから（必ずしも最も古いメッセージからとは限りません）、新しいメッセージに十分な領域が空くまで、メッセージが解放されていきます。オーバーフローのためにメッセージが解放される前に、添付ファイルの削除、件名の変更、X-Header の追加といったアクションがメッセージに対して実行されるように、Outbreak 検疫を設定できます。

検疫されているメッセージは、新しいルールが発行されるたびに再スキャンされるため、Outbreak 検疫エリアにあるメッセージは有効期限が切れる前に解放されることがほとんどです。

それでも、デフォルト アクションが「削除」に設定されている場合は、Outbreak 検疫をモニタすることが重要です。IronPort は、ほとんどのユーザに対して、デフォルト アクションを「削除」に設定しないことを推奨します。Outbreak 検疫エリアからのメッセージの解放、または Outbreak 検疫のデフォルト アクションの変更に関する詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。

反対に、新しいウイルス定義を待つ間、Outbreak 検疫エリアに長時間留めておきたいメッセージがある場合は、たとえばそのメッセージの有効期限を遅らせることもできます。メッセージの保持期間を増やすことにより、検疫エリアのサイズが大きくなる場合があるため、注意してください。

（注） メッセージが Outbreak 検疫エリアに留まっている間にアンチウイルス スキャンが（メール ポリシーごとではなく）グローバルにディセーブルにされた場合は、たとえメッセージが解放される前にもう一度アンチウイルス スキャンを再度イネーブルにしたとしても、そのメッセージが解放されたときのアンチウイルス スキャンは実行されません。

（注） ウイルス感染フィルタ機能は、IronPort アプライアンスでアンチウイルス スキャンをイネーブルにしなくても使用できます（「検疫およびアンチウイルス スキャン」（P.10-340）を参照）。

[Outbreak Quarantine] および [Manage by Rule Summary] ビュー

GUI の [Monitor] メニューにあるリスト内の検疫名をクリックすることで、その他のすべての検疫と同様に、Outbreak 検疫エリアの内容を表示できます。Outbreak 検疫には、追加のビューである、Outbreak 検疫の [Manage by Rule Summary] リンクもあります。

図 10-8　Outbreak 検疫の [Manage by Rule Summary] リンク

Quarantines

Quarantine Overview

Add Quarantine...

Quarantine Name	Search	# of Messages	% Full	Space Allocation	Retention Period	Action	Users	Settings	Delete
Outbreak [Manage by Rule Summary]		4	0.0	3,072 MB	12h	Release		Edit	
Policy		974	0.1	1,024 MB	10d	Delete		Edit	
Virus		8	0.0	2,048 MB	30d	Delete		Edit	

サマリー ビューの使用による Outbreak 検疫エリア内のメッセージに対するルール ID に基づいたメッセージ アクションの実行

[Manage by Rule Summary] リンクをクリックして、ルール ID ごとにグループ化された Outbreak 検疫の内容のリストを表示します。

図 10-9　Outbreak 検疫の [Manage by Rule Summary] ビュー

Outbreak Quarantine Summary

Manage by Rule Summary

All Select	Rule ID	Number of messages	Average message size	Total size	Capacity
	EXE_BAGL	4	16 KB	0.1 MB	0.0%
	Totals	4	16 KB		

Select Action... Submit

個別にメッセージを選択しなくても、このビューから特定のアウトブレイクまたはアダプティブ ルールに関するすべてのメッセージに対して、解放、削除、または保持期間延長を実行するように選択できます。また、検索またはリストのソートも実行できます。

この機能は、`quarantineconfig -> vofmanage` CLI コマンドからも使用できます。詳細については、『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください。

ウイルス感染フィルタのモニタリング

IronPort Systems は、ウイルス感染フィルタ機能のパフォーマンスおよび活動をモニタするツールを複数提供しています。

ウイルス感染フィルタの概要とルール リスト

概要およびルール リストは、ウイルス感染フィルタ機能の現在の状態に関して役立つ情報を提供します。この情報は、[Security Services] > [Virus Outbreak Filters] ページで表示します。

Outbreak 検疫

Outbreak 検疫を使用して、現在どの位のメッセージがウイルス感染フィルタの脅威レベルのしきい値により、フラグ付けされているかモニタします。また、ルールごとの検疫メッセージのリストも使用できます。この情報は、[Monitor] > [Local Quarantines] > [Outbreak] リンクおよび [Monitor] > [Local Quarantines] ページの [Manage Rule by Summary] リンクで表示します。

サポート Web サイト

IronPort Systems は、アプライアンス以外でも役立つ情報を提供しています。次の URL には、ウイルス アウトブレイクおよびウイルス感染フィルタ機能に関連する情報、ステータス、およびウイルス脅威の詳細が含まれています。

`http://www.ironport.com/`（Virus Threat Level チャート）

`http://www.ironport.com/`（ウイルス脅威の詳細）

`https://support.ironport.com/index_.html`（ウイルス アウトブレイクに関する情報）

アラート、SNMP トラップ、およびウイルス感染フィルタ

ウイルス感染フィルタ機能は、定期的な AsyncOS アラートと SNMP トラップという 2 つの異なるタイプの通知をサポートしています。

SNMP トラップは、ルールのアップデートが失敗したときに作成されます。AsyncOS の SNMP トラップの詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Managing and Monitoring via the CLI」の章を参照してください。

AsyncOS のウイルス感染フィルタ機能には、2 つのタイプのアラート（サイズおよびルール）が用意されています。

AsyncOS アラートは、Outbreak 検疫エリアのサイズが最大サイズの 5、50、75、および 95 を超えるたびに生成されます。95 % のしきい値を超えたときに生成されるアラートの重大度は CRITICAL、その他のアラートしきい値の場合は WARNING です。アラートは、検疫エリアのサイズが大きくなり、しきい値を超えたときに生成されます。検疫エリアのサイズが小さくなり、しきい値を下回ったときは生成されません。アラートの詳細については、「アラート」（P.15-495）を参照してください。

また、AsyncOS はルールが発行されたとき、しきい値が変更されたとき、またはルールまたは CASE エンジンのアップデート中に問題が発生したときにもアラートを生成します。

ウイルス感染フィルタ機能のトラブルシューティング

このセクションでは、ウイルス感染フィルタ機能の基本的なトラブルシューティングに関するヒントをいくつか紹介します。

[Manage Quarantine] ページのチェックボックスを使用すると、Outbreak 検疫が IronPort に対して誤分類を通知するようになります。

任意で、次の電子メール アドレスを使用して、IronPort Systems に誤分類をレポートできます。

- clean@ironport.com
- outbreaks@ironport.com（調査用に Outbreak 検疫エリアに送信したメッセージのレポート用）

複数の添付ファイルおよびバイパスされるファイル タイプ

バイパスされるファイル タイプは、メッセージに 1 つだけ添付されているファイルのタイプが指定したタイプであった場合、または、メッセージに複数のファイルが添付されている場合は、その他の添付ファイルに対して既存のルールが存在しない場合のみ、除外されます。これ以外の場合は、メッセージはスキャンされます。

メッセージ フィルタ、コンテンツ フィルタ、および電子メール パイプライン

メッセージ フィルタおよびコンテンツ フィルタは、ウイルス感染フィルタによるスキャンが実行される前にメッセージに適用されます。フィルタを適用することにより、メッセージがウイルス感染フィルタ スキャンをスキップしたり、バイパスしたりする場合があります。