アウトブレイク フィルタ

この章は、次の項で構成されています。

- アウトブレイク フィルタの概要 （1 ページ）
- アウトブレイク フィルタの動作 （2 ページ）
- アウトブレイク フィルタの機能概要 （10 ページ）
- アウトブレイク フィルタの管理 （14 ページ）
- アウトブレイク フィルタのモニタリング （27 ページ）
- アウトブレイク フィルタ機能のトラブルシューティング （28 ページ）

アウトブレイク フィルタの概要

アウトブレイク フィルタは大規模なウイルスの拡散、および小規模のフィッシング詐欺およびマルウェア配布といった、非ウイルス性の攻撃が発生した際にネットワークを保護します。データが収集され、ソフトウェアの更新が公開されるまで新たな拡散を検知できない通常のアンチマルウェア セキュリティ ソフトウェアとは異なり、シスコは感染が拡散したときにデータを収集し、ユーザにこれらのメッセージが到達することを防ぐためにリアルタイムでEメール セキュリティ アプライアンスに更新情報を送信します。

シスコは着信メッセージは、着信メッセージが安全またはアウトブレイクの一部であることを判断するルールを開発するためにグローバル トラフィック パターンを使用します。アウトブレイクの一部となる可能性があるメッセージは、シスコからアップデートされたアウトブレイクの情報またはSophosおよびMcAfeeによって発行される新しいアンチウイルス定義に基づいて安全と判断されるまで隔離されます。

小規模な非ウイルス性の攻撃で使用されるメッセージは、正当に見える外見、受信者情報、そして短期間だけオンラインに存在し Web セキュリティ サービスが知らないフィッシングおよびマルウェア Web サイトを参照するカスタム URL を使用します。アウトブレイク フィルタはメッセージの内容を分析し、この種の非ウイルス性の攻撃を検出するために URL リンクを検索します。アウトブレイク フィルタは Web セキュリティ プロキシによって潜在的に危険な Web サイトへのトラフィックをリダイレクトするために URL を書き換え、ユーザがアクセスしようとしている Web サイトが悪意があるかもしれないことを警告するかまたは Web サイトを完全にブロックします。

アウトブレイク フィルタの動作

関連項目

- メッセージの遅延、リダイレクトおよび修正 （2 ページ）
- 脅威カテゴリ （2 ページ）
- Cisco Security Intelligence Operations （4 ページ）
- コンテキスト適応スキャン エンジン （4 ページ）
- メッセージの遅延 （5 ページ）
- URL のリダイレクト （5 ページ）
- メッセージの変更 （7 ページ）
- 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 （7 ページ）
- アウトブレイク （8 ページ）
- 脅威レベル （8 ページ）

メッセージの遅延、リダイレクトおよび修正

アウトブレイク フィルタ機能は、ウイルス感染からユーザを保護するために3つの戦略を使用します。

- **遅延。**アウトブレイク フィルタは、ウイルス感染の一部または非ウイルス性の攻撃である可能性のあるメッセージを隔離します。隔離の間、アプライアンスはアップデートされたアウトブレイク情報を受信し、攻撃の一部であるかどうか確認するためにメッセージを再スキャンします。
- **リダイレクト。**リンクされた Web サイトのいずれかにアクセスしようとすると、Cisco Web セキュリティ プロキシによって受信者をリダイレクトするように非ウイルス性の攻撃のメッセージ内の URL を書き換えます。プロキシは、Web サイトがまだ動作中である場合は、その Web サイトにマルウェアが含まれる可能性があることをユーザに警告するスプラッシュ画面を表示し、Web サイトがオフラインになっている場合は、エラー メッセージを表示します。URL のリダイレクトの詳細については、URL のリダイレクト （5 ページ）を参照してください。
- **変更。**非ウイルス性の脅威メッセージの URL 書き換えに加えて、アウトブレイク フィルタはユーザにメッセージの内容についてユーザに警告するためにメッセージの件名を変更して、メッセージ本文の上に免責事項を追加できます。詳細については、メッセージの変更 （7 ページ）を参照してください。

脅威カテゴリ

アウトブレイク フィルタ機能は、メッセージに基づくアウトブレイクの次の2つのカテゴリからの保護を提供します。ウイルス アウトブレイクは、添付ファイルに見たことのないウイルスが含まれるメッセージで、非ウイルス性の脅威には、外部 Web サイトへのリンクを経由するフィッシング試行、詐欺、およびマルウェア配布が含まれます。

デフォルトでアウトブレイク フィルタ機能は、アウトブレイク中の可能性があるウイルスがあるかどうか送受信メッセージをスキャンします。アプライアンスでアンチスパム スキャンをイネーブルにする場合は、ウイルス アウトブレイクに加えて、非ウイルス性の脅威のスキャンをイネーブルにできます。

（注） アウトブレイク フィルタが非ウイルス性の脅威をスキャンするために、Anti-Spam または Intelligent Multi-Scan のライセンス キーが必要です。

関連項目

- ウイルス アウトブレイク （3 ページ）
- フィッシング、マルウェア配布、およびその他の非ウイルス性の脅威 （3 ページ）

ウイルス アウトブレイク

アウトブレイク フィルタ機能を使用することで、ウイルス アウトブレイク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。アウトブレイクは、見たことのないウイルスまたは既存のウイルスの変異型を含む添付ファイルを持つメッセージがプライベート ネットワークおよびインターネットを経由してすばやく拡散するときに発生します。これらの新しいウイルスまたはウイルスの変異型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、マルウェアまたはウイルスの拡散を抑えるうえで非常に重要です。ウイルス定義がリリースされるまでの間に、新しく発見された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。

フィッシング、マルウェア配布、およびその他の非ウイルス性の脅威

非ウイルス性の脅威を含んでいるメッセージは、正規の送信元からのメッセージのように設計されていて、多くの場合、少数の受信者に送信されます。これらのメッセージには、信頼できると見せるために次の 1 つまたは複数の特徴がある場合があります。

- 受信者の連絡先情報。
- HTML コンテンツは、ソーシャル ネットワークおよびオンライン販売などの正規の送信元からの電子メールを模倣するように設計されています。
- 新しい IP アドレスを持ち、短期間だけオンラインである Web サイトを指している URL。これは電子メールおよび Web セキュリティ サービスに、その Web サイトが不正かどうか判断するための十分な情報がないことを意味します。
- URL 短縮サービスを指している URL。

これらの特徴すべてによって、これらのメッセージをスパムとして検出するのがさらに難しくなります。アウトブレイク フィルタ機能によって、これらの非ウイルス性の脅威に対するマルチレイヤの防衛が提供され、ユーザがマルウェアをダウンロードしたり、個人情報を新しい不審な Web サイトに提供したりすることを防ぎます。

CASE はメッセージ内に URL を発見すると、そのメッセージを既存のアウトブレイク ルールと比較して、そのメッセージが小規模の非ウイルス性のアウトブレイクの一部かどうか判断し、次に脅威レベルを割り当てます。脅威レベルに応じて、E メール セキュリティ アプライアンスは、より多くの脅威のデータを集められるまで受信者への配信を遅らせ、Web サイトにアクセスしようとすると Cisco Web セキュリティ プロキシへ受信者をリダイレクトするようにメッセージ内の URL を書き換えます。プロキシは、その Web サイトにマルウェアが含まれる可能性があることをユーザに警告するスプラッシュ ページを表示します。

Cisco Security Intelligence Operations

Cisco Security Intelligence Operations（SIO）は、グローバルな脅威情報、レピュテーションに基づくサービス、および高度な分析を Cisco セキュリティ アプライアンスに結び付け、より強力な保護をより迅速な応答時間で提供するセキュリティ エコシステムです。

SIO は次の 3 種類のコンポーネントからなります。

- SenderBase。世界有数の規模を誇る脅威モニタリング ネットワークおよび脆弱性データベース。
- Threat Operations Center（TOC）。セキュリティ専門家のグローバル チームおよび SenderBase によって収集された実行可能な情報を抽出する自動システム。
- Dynamic Update。アウトブレイク発生時に、アプライアンスに自動的に配信されるリアルタイムの更新。

SIO は、グローバル SenderBase ネットワークからのリアルタイム データを、共通のトラフィック パターンと比較して、アウトブレイクの確かな前兆である異常を識別します。TOC は、データをレビューしてアウトブレイクの可能性の脅威レベルを発行します。Cisco E メール セキュリティ アプライアンスは、アップデートされた脅威レベルとアウトブレイク ルールをダウンロードし、それらを使用してすでにアウトブレイク隔離エリアにあるメッセージと同様に送受信メッセージをスキャンします。

現在のウイルス アウトブレイクに関する情報は、次の SenderBase の Web サイトで入手できます。

http://www.senderbase.org/

次の SIO Web サイトに、スパム、フィッシング、およびマルウェア配布の試行を含む現在の非ウイルス性の脅威のリストが記載されています。

http://tools.cisco.com/security/center/home.x

コンテキスト適応スキャン エンジン

アウトブレイク フィルタには、シスコ独自のコンテキスト適応スキャン エンジン（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 アウトブレイクの場合、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 SIO 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、各メッセージを評価し、独自の脅威レベルを割り当てます。

非ウイルス性の脅威を検出するために、CASE は URL に対してメッセージをスキャンし、1 つまたは複数の URL が発見されると SIO が提供するアウトブレイク ルールを使用してメッセージの脅威レベルを評価します。

メッセージの脅威レベルに基づいて、CASE は、アウトブレイクを防ぐためにメッセージを一定期間隔離することを推奨します。SIO が提供するアップデートされたアウトブレイク ルールに基づいてメッセージを再評価できるように、CASE は再スキャンの間隔も決定します。脅威レベルが高くなるほど、隔離中のメッセージの再スキャンの頻度が高くなります。

メッセージが隔離解除されるときに、CASE はメッセージの再スキャンも行います。再スキャン時に、CASE によりメッセージがスパムであるか、ウイルスを含むと判断された場合、メッセージを再度隔離できます。

CASE の詳細については、Cisco Anti-Spam：概要を参照してください。

メッセージの遅延

アウトブレイクまたは電子メール攻撃の発生と、ソフトウェア ベンダーによるアップデートしたルールのリリースの間の期間は、ネットワークとユーザが最も脆弱なときです。この期間に、現代のウイルスはグローバルに伝播でき、また不正な Web サイトはマルウェアを配信したり、ユーザの機密情報を収集したりすることができます。限られた期間に疑わしいメッセージを隔離することによって、アウトブレイク フィルタは、ユーザおよびネットワークを保護し、シスコおよびその他のベンダーに新しいアウトブレイクを調査する時間を与えます。

ウイルス アウトブレイクが発生すると、アップデートされたアウトブレイク ルールおよび新しいアンチウイルス シグニチャにより、その電子メールの添付ファイルがクリーン、またはウイルスであることが証明されるまで添付ファイルを含む疑わしいメッセージは隔離されます。

小規模の非ウイルス性の脅威には、Web セキュリティ サービスによる検出を回避するために短期間オンラインになる可能性のある不正な Web サイトへの URL、または Web セキュリティを回避するため、信頼できる Web サイトを途中に置いて URL 短縮サービスを経由する URL が含まれます。脅威レベルのしきい値を満たす URL を含んでいるメッセージの隔離によって、CASE は SIO が提供するアップデートされたアウトブレイク ルールに基づいてメッセージの内容を再評価できるだけでなく、リンクされた Web サイトがオフラインになるか、Web セキュリティ ソリューションによってブロックできるほど長く、メッセージを隔離のままにしておくことができます。

疑いのあるメッセージに対するアウトブレイク フィルタの隔離方法の詳細については、動的隔離 （12 ページ）を参照してください。

URL のリダイレクト

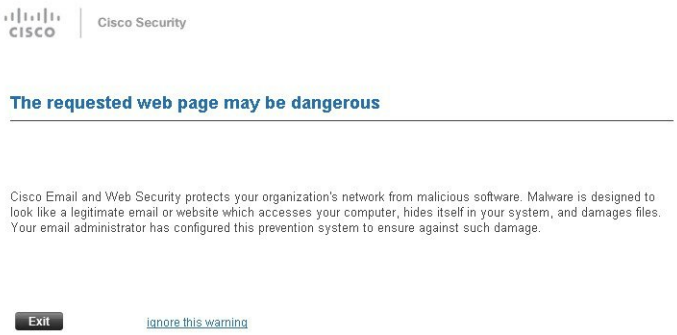
CASE がアウトブレイク フィルタの段階でメッセージをスキャンする場合、他の疑わしい内容に加えてメッセージ本文に URL があるかどうか検索します。CASE は、発行されたアウトブレイク ルールを使用して、そのメッセージが脅威であるかどうかを評価して、次に適切な脅威

レベルでメッセージをスコアリングします。脅威レベルに応じて、アウトブレイク フィルタは、受信者が Cisco Web セキュリティ プロキシにリダイレクトされるように、バイパスされたドメインを指している URL を除くすべての URL を書き換えることによって受信者を保護します。メッセージがより大きなアウトブレイクの一部であると思われる場合は、TOC が Web サイトについてさらに詳しく調べるためにメッセージの配信を遅らせます。信頼ドメインへの URL のバイパスの詳細については、URL 書き換えおよびドメインのバイパス （23 ページ）を参照してください。

E メール セキュリティ アプライアンスがメッセージをリリースおよび配信した後で、受信者による Web サイトへのアクセスの試行があれば、Cisco Web セキュリティ プロキシによってリダイレクトされます。これは、シスコによってホストされている外部プロキシで、Web サイトが引き続き使用可能な場合、その Web サイトが危険である可能性があることをユーザに警告するスプラッシュ画面を表示します。Web サイトがオフラインになった場合は、スプラッシュ画面にエラー メッセージが表示されます。

受信者がメッセージの URL をクリックすることにした場合、Cisco Web セキュリティ プロキシは、ユーザの Web ブラウザにスプラッシュ画面を表示して、メッセージの内容について警告します。次の図は、スプラッシュ画面の警告の例を示しています。受信者は、[この警告を無視する（Ignore this warning）] をクリックして Web サイトへ進むか、[終了（Exit）] をクリックして退出し、ブラウザ ウィンドウを安全に閉じることができます。

図 *1:* シスコのセキュリティによるスプラッシュ画面の警告（*proxy_splash_screen*）



Cisco Web セキュリティ プロキシにアクセスする唯一の方法は、メッセージ内の URL を書き換えることです。Web ブラウザで URL を入力しても、プロキシにはアクセスできません。

（注） このスプラッシュ画面の外観をカスタマイズして、会社のロゴ、連絡先情報などの自社のブランディングを表示することができます。サイトに悪意がある場合にエンドユーザに表示する通知のカスタマイズを参照してください。

ヒント スパムの可能性があるメッセージの URL をすべて Cisco Web セキュリティ プロキシ サービスにリダイレクトするには、カスタム ヘッダーを使用して、陽性と疑わしいスパム内の URL を Cisco Web セキュリティ プロキシにリダイレクトする：設定例を参照してください。

メッセージの変更

アウトブレイク フィルタ機能は、非ウイルス性の脅威であるメッセージのメッセージ本文を変更して、URL を書き換えるだけでなく、メッセージが疑わしい脅威であるというアラートをユーザに出します。アウトブレイク フィルタ機能は、件名ヘッダーを変更したり、メッセージ本文上部にメッセージの内容について免責事項を追加したりできます。詳細については、メッセージ変更 （21 ページ）を参照してください。

脅威の免責事項は、[メールポリシー（Mail Policies）] > [テキストリソース（Text Resources）] ページから免責事項テンプレートを使用して作成されます。詳細については、テキストリソース管理の概要を参照してください。

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

アウトブレイク フィルタでは、アダプティブ ルールおよびアウトブレイク ルールの 2 つのタイプのルールを使用して、潜在的なアウトブレイクを検出します。アウトブレイク フィルタ機能は、これらの2つのルールセットを使用して、高い有効性を持ち、綿密に的を絞った、一連の脅威検出基準を提供することで、フィルタが確実に特定のアウトブレイク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。アウトブレイク 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、隔離されたメッセージにただちにアクセスしたり、隔離された理由を確認したりできるようになっています。

関連項目

- 適応ルール （8 ページ）
- アウトブレイクのルール （7 ページ）

アウトブレイクのルール

アウトブレイク ルールは、Cisco Security Intelligence Operations の一部である、Cisco 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（たとえばアウトブレイク隔離など）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。TOC は、データをレビューして脅威のインジケータまたは脅威レベルを発行します。脅威レベルは 0（脅威なし）から 5（非常に危険）の範囲の数値で表し、メッセージがシスコのお客様による他のゲートウェイの防御が広く導入されていない脅威である可能性を判断します（詳細については、脅威レベル （8 ページ）を参照してください）。脅威レベルは、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

適応ルール

アダプティブ ルールは、CASE内の一連のルールであり、メッセージの属性を既知のウイルス アウトブレイク メッセージの属性と正確に比較します。これらのルールは、広範なウイルス コーパスの中で、既知の脅威の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。

アウトブレイク

アウトブレイク フィルタ ルールは、基本的に、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）に関連付けられた脅威レベル（例：4）です。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、Cisco SIO 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脅威レベルを上げたアウトブレイク ルールが発行されます。デフォルトでは、アプライアンスは、新しく発行されたアウトブレイク ルール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（アウトブレイク フィルタ ルールのアップデート （19 ページ）を参照）。アダプティブ ルールは、アウトブレイク ルールほど頻繁にはアップデートされません。アプライアンスで、疑わしいメッセージの隔離についてしきい値を設定します。メッセージの脅威レベルが隔離のしきい値以上の場合、メッセージはアウトブレイク 隔離エリアに送信されます。非ウイルス性の脅威のメッセージの変更についてしきい値を設定して、疑わしいメッセージで発見されたURLすべてを書き換えたり、メッセージ本文の上部に通知を追加したりできます。

脅威レベル

次の表に、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。

水準器	リスク	意味
[0]	なし	メッセージが脅威であるリスクはありません。
1	低（Low）	メッセージが脅威であるリスクは低です。
2	低または中	メッセージが脅威であるリスクは低から中です。これは「疑わしい」脅威です。
3	中	メッセージが確認されているアウトブレイクの一部であるか、メッセージの内容が脅威である中から高のリスクがあります。
4	高	メッセージが大規模アウトブレイクの一部であることが確認されているか、メッセージの内容が非常に危険です。
5	最高	メッセージの内容が、非常に大規模または大規模な、かつ非常に危険なアウトブレイクの一部であることが確認されています。

脅威レベルおよびアウトブレイク ルールの詳細については、アウトブレイク フィルタ ルール（18 ページ）を参照してください。

関連項目

- 隔離脅威レベルのしきい値設定ガイドライン （9 ページ）
- コンテナ：特定ルールおよび常時ルール （9 ページ）

隔離脅威レベルのしきい値設定ガイドライン

隔離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隔離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隔離されます。反対に、高いスコア（4 または 5）は消極的な設定値で、不正である可能性がきわめて高いメッセージのみが隔離されます。

ウイルスアウトブレイクおよび非ウイルス性の脅威の両方に同じしきい値が適用されますが、ウイルス攻撃およびその他の脅威に対して、異なる隔離の保持期間を指定できます。詳細については、動的隔離 （12 ページ）を参照してください。

シスコは、デフォルト値の 3 を推奨します。

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 zip（.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、TOC により、あるウイルス アウトブレイクが、1 つの .exe を含む 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)）に脅威レベルを設定する特定のアウトブレイク ルールが発行されます。ただし .zip ファイル内に含まれるその他のファイル 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ません。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、メッセージの脅威レベル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 SIO により発行されます。

表 *1:* 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。

アウトブレイク フィルタの機能概要

電子メール メッセージは、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 パイプラインについて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するので、これらのエンジンがメール ポリシーをイネーブルにしている場合、アンチスパムおよびアンチウイルス スキャンを実行します。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、アウトブレイク 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、隔離など）されているため、アウトブレイク フィルタ機能ではスキャンされません。このため、アウトブレイク フィルタ機能に到達するメッセージは、スパムおよびウイルスを含まないとマークされています。アウトブレイク フィルタによって隔離されたメッセージは、CASEによって隔離解除されて、再スキャンされる際、アップデートされたスパム ルールおよびウイルス定義に基づいて、スパムまたはウイルスを含んでいるとしてマークされる可能性があることに注意してください。

（注） フィルタおよびエンジンがディセーブルになっていることでアンチスパムおよびアンチウイルス スキャンをスキップするメッセージでも、アウトブレイク フィルタによってスキャンされます。

関連項目

- メッセージ スコアリング （11 ページ）
- 動的隔離 （12 ページ）

メッセージ スコアリング

新しいウイルス攻撃または非ウイルス性の脅威がコンピュータ ネットワークに放たれた時点では、脅威を認識できるアンチウイルスやアンチスパム ソフトウェアはまだありません。アウトブレイク 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、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を使用して、CASEによりスキャンおよびスコアリングされます（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 （7 ページ）を参照）。メッセージ スコアはメッセージの脅威レベルに対応しています。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、CASE は対応する脅威レベルを割り当てます。関連する脅威レベルが存在しない（メッセージに一致するルールが存在しない）場合は、メッセージには脅威レベル 0 が割り当てられます。

その計算が完了すると、E メール セキュリティ アプライアンスは、メッセージの脅威レベルが隔離またはメッセージ変更のしきい値以上であるかどうかをチェックし、メッセージを隔離するかメッセージの URL を書き換えます。脅威レベルがしきい値を下回る場合、パイプラインの後続の処理が継続されます。

さらに、CASE は既存の隔離されているメッセージを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隔離され続け、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隔離エリアから解放されます。

1 つのアウトブレイク メッセージで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最終的な脅威レベルが決定されます。

アウトブレイク フィルタ機能は、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、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、アウトブレイク隔離エリアにあるメッセージの一部を手動で隔離解除したり、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アウトブレイク 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 ルールに従って隔離されます。
- 脅威レベルが引き下げられたり、隔離時間の期限が過ぎたりした場合は、メッセージは隔離解除されます。

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/グループウェア）は、隔離解除されたメッセージを捕捉する場合があります。

（注） アウトブレイク フィルタ機能が非ウイルス性の脅威をスキャンするために、アンチスパム スキャンをアプライアンスでグローバルにイネーブルにする必要があります。

動的隔離

アウトブレイク フィルタ機能のアウトブレイク隔離エリアは、メッセージが脅威であると確認されるか、ユーザに配信しても安全であることが確認されるまで、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 （13 ページ）を参照してください）。隔離されたメッセージは、複数の方法でアウトブレイク隔離エリアから解放できます。新しいルールがダウンロードされると、アウトブレイク隔離エリアにあるメッセージは、CASE によって計算された推奨再スキャン間隔に基づいて再評価されます。更新されたメッセージの脅威レベルが隔離保持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（アウトブレイク隔離の設定に関係なく）隔離解除されるため、メッセージが隔離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。

ウイルス攻撃として隔離されるメッセージは、新しいアンチウイルス シグニチャが使用可能な場合は、自動的にアウトブレイク隔離エリアからリリースされることはないため、注意してください。新しいルールは、新しいアンチウイルス シグニチャ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、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、メッセージが隔離解除されることはありません。

CASE の推奨保持期間が経過した場合も、メッセージはアウトブレイク隔離エリアから解放されます。CASE は、メッセージの脅威レベルに基づいて保持期間を計算します。ウイルス アウトブレイクおよび非ウイルス性の脅威に対して別々の最大保持期間を定義できます。CASE の推奨保持期間がその脅威タイプの最大保持期間を超える場合、E メール セキュリティ アプライアンスは、最大保持期間が経過した時点でメッセージを解放します。ウイルス性のメッセージのデフォルトの最大隔離期間は 1 日です。非ウイルス性の脅威を隔離するデフォルト期間は 4 時間です。メッセージを、手動で隔離解除できます。

また、隔離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 E メール セキュリティ アプライアンスもメッセージをリリースします（これはオーバーフローと呼ばれます）。オーバーフローは、アウトブレイク隔離エリアが容量の 100 % まで使用されているときに、新しいメッセージが隔離エリアに追加された場合のみ発生します。このとき、メッセージが隔離解除される優先順位は次のとおりです。

- アダプティブ ルールにより隔離されたメッセージ（最も早く隔離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 ルールにより隔離されたメッセージ（最も早く隔離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）

アウトブレイク隔離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。隔離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、隔離内のメッセージの保持期間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 アクションを参照してください。

アウトブレイク隔離エリアから解放されたメッセージは、アンチウイルスおよびアンチスパム エンジンがメール ポリシーでイネーブルとなっている場合、アンチウイルスおよびアンチスパム エンジンによって再度スキャンされます。このときに既知のウイルスまたはスパムとしてマークされた場合は、このメッセージはメール ポリシー設定に従って処理されます（ウィルス

隔離エリアまたはスパム隔離エリアに隔離される場合もあります）。詳細については、アウトブレイク フィルタ機能とアウトブレイク隔離 （24 ページ）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 回隔離される場合がある（1 回はアウトブレイク フィルタ機能により、もう 1 回はアウトブレイク隔離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。各スキャン（アウトブレイク フィルタの前およびアウトブレイク隔離エリアから解放されたとき）照合の結果、何らかの判断がなされたメッセージは、2 回隔離されることはありません。また、アウトブレイク 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。アウトブレイク フィルタ機能は、（後続の処理のために）メッセージを隔離するか、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。

関連項目

- アウトブレイク ライフサイクルおよびルール発行 （13 ページ）

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、メッセージを隔離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、隔離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、隔離解除されます（アウトブレイク隔離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 *2:* アウトブレイク ライフサイクルのルールの例

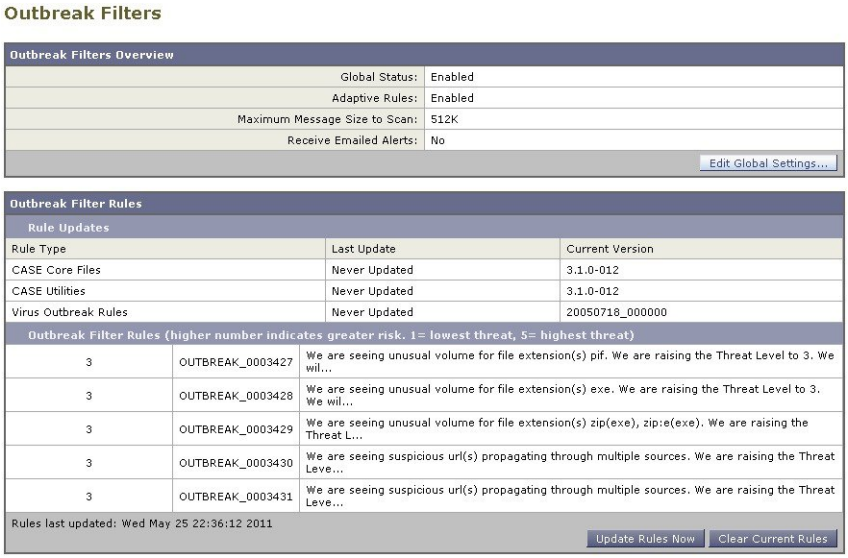
時間	ルール タイプ	ルールの説明	操作
T=0	アダプティブ ルール（過去のアウトブレイクに基づく）	10 万を超えるメッセージ属性に基づく、統合されたルール セットで、メッセージの内容、コンテキスト、および構造を分析します。	アダプティブ ルールに一致したメッセージは、自動的に隔離されます。
T=5 分	アウトブレイク ルール	.zip（exe）ファイルが含まれるメッセージを隔離します。	.exe が含まれる .zip 形式の添付ファイルはすべて隔離されます。
T=10 分	アウトブレイク ルール	50 KB を超える .zip（exe）ファイルが含まれるメッセージを隔離します。	50 KB 未満の .zip（exe）ファイルが含まれたメッセージはすべて隔離解除されます。
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隔離します。	この基準に一致しないメッセージはすべて隔離解除されます。

時間	ルール タイプ	ルールの説明	操作
T=12 時間	アウトブレイク ルール	新しいシグニチャ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 シグニチャを使用してスキャンします

アウトブレイク フィルタの管理

グラフィカル ユーザ インターフェイス（GUI）にログインし、メニューの [セキュリティ サービス（Security Services）] を選択して、[アウトブレイクフィルタ（Outbreak Filters）] をクリックします。

図 *2 : [アウトブレイク フィルタ（Outbreak Filters）] メインページ*



[アウトブレイクフィルタ（Outbreak Filters）] ページには、[アウトブレイクフィルタの概要（Outbreak Filters Overview）] と現在の [アウトブレイクフィルタのルール（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。

上の図で、アウトブレイク フィルタはイネーブル、Adaptive Scanning はイネーブル、また最大メッセージ サイズは 512 K に設定されています。これらの設定を変更するには、[グローバル設定を編集（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、アウトブレイク フィルタのグローバル設定の構成 （15 ページ）を参照してください。

[アウトブレイクフィルタのルール（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、脅威レベルと共にアウトブレイク 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、アウトブレイク フィルタ ルール （18 ページ）を参照してください。

関連項目

- アウトブレイク フィルタのグローバル設定の構成 （15 ページ）
- アウトブレイク フィルタ ルール （18 ページ）
- アウトブレイク フィルタ機能とメール ポリシー （19 ページ）
- アウトブレイク フィルタ機能とアウトブレイク隔離 （24 ページ）

アウトブレイク フィルタのグローバル設定の構成

ステップ 1 [セキュリティ サービス（Security Services）] > [アウトブレイク フィルタ（Outbreak Filters）] をクリックします。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 要件に応じて、次を実行します。

- アウトブレイク フィルタをグローバルにイネーブルにします。
- アダプティブ ルールのスキャンをイネーブルにします。
- スキャンするファイルの最大サイズを設定します（サイズをバイトで入力することに注意してください）。
- アウトブレイク フィルタのアラートをイネーブルにします。
- Web インタラクション トラッキングをイネーブルにします。Web インタラクション トラッキングを参照してください。

ステップ 4 変更を送信し、保存します。

次のタスク

この機能は、outbreakconfig CLI コマンドによっても使用可能です（『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』を参照）。変更を加えたら、送信して確定します。

（注） Webインターフェイスを使用してURLのロギングをイネーブルにすることはできません。CLIを使用して URL のロギングをイネーブルにする手順については、URL のロギングと URL のメッセージ トラッキングの詳細の有効化 （17 ページ）を参照してください。

関連項目

- アウトブレイク フィルタ機能の有効化 （16 ページ）
- アダプティブ ルールの有効化 （16 ページ）
- アウトブレイク フィルタのアラートの有効化 （16 ページ）

• URL のロギングと URL のメッセージ トラッキングの詳細の有効化 （17 ページ）

アウトブレイク フィルタ機能の有効化

アウトブレイク フィルタ機能をグローバルに有効にするには、[アウトブレイクフィルタのグローバル設定（Outbreak Filters Global Settings）] ページの [アウトブレイクフィルタを有効にする（Enable Outbreak Filters）] の横にあるボックスをオンにして、[送信（Submit）] をクリックします。事前にアウトブレイク フィルタ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、アウトブレイク フィルタ機能は、各送受信メール 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、アウトブレイク フィルタ機能とメール ポリシー （19 ページ）を参照してください。

アウトブレイク フィルタ機能は、アンチスパム 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、コンテキスト適応スキャン エンジン（CASE）を使用してウイルス性の脅威を検出します。ただし、非ウイルス性の脅威をスキャンするために、アプライアンスで Anti-Spam または Intelligent Multi-Scan をグローバルにイネーブルにする必要があります。

（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：セキュリティを参照）は、[セキュリティサービス（Security Services）]>[アウトブレイクフィルタ（Outbreak Filters）] ページで [有効（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 ルールの有効化

Adaptive Scanning は、アウトブレイク フィルタのアダプティブ ルールをイネーブルにします。メッセージの内容に関するウイルス シグニチャまたはスパム基準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、メッセージがアウトブレイクの一部である可能性が決定されます。Adaptive Scanning を有効にするには、[アウトブレイクフィルタのグローバル設定（Outbreak Filters Global Settings）] ページの [適応ルールを有効にする（Enable Adaptive Rules）] の横にあるボックスをオンにして、[送信（Submit）] をクリックします。

アウトブレイク フィルタのアラートの有効化

[アラート メール（Emailed Alerts）] というラベルの付いたボックスをオンにして、アウトブレイク フィルタ機能のアラートをイネーブルにします。アウトブレイク 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、アウトブレイク 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、[アラート（Alerts）] ページの [システム管理（System Administration）] タブで設定します。アウトブレイク 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、およびアウトブレイク フィルタ （28 ページ）を参照してください。

URL のロギングと URL のメッセージ トラッキングの詳細の有効化

URL 関連のログのログ収集と、メッセージ トラッキングの詳細のこの情報の表示は、デフォルトで無効になっています。これには、次のイベントのログが含まれます。

- メッセージ内の特定の URL のカテゴリが URL カテゴリ フィルタと一致した
- メッセージ内の特定の URL のレピュテーション スコアが URL レピュテーション フィルタと一致した
- アウトブレイク フィルタによってメッセージ内の特定の URL が書き換えられた

これらのイベントのログ収集を有効にするには、コマンドライン インターフェイス（CLI）で outbreakconfig コマンドを使用します。

関連項目

- 例：outbreakconfig コマンドを使用して URL のロギングを有効にする （17 ページ）
- アウトブレイク フィルタ ルールの管理 （18 ページ）
- 例：outbreakconfig コマンドを使用して URL のロギングを有効にする （17 ページ）

例：outbreakconfig コマンドを使用して URL のロギングを有効にする

次に、outbreakconfig コマンドを使用して URL のロギングをイネーブルにする例を示します。

```
mail.example.com> outbreakconfig

Outbreak Filters: Enabled

Choose the operation you want to perform:

- SETUP - Change Outbreak Filters settings.

[]> setup

Outbreak Filters: Enabled

Would you like to use Outbreak Filters? [Y]>

Outbreak Filters enabled.

Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or
back down below), meaning that new messages of

certain types could be quarantined or will no longer be quarantined, respectively.

Would you like to receive Outbreak Filter alerts? [N]>

What is the largest size message Outbreak Filters should scan?

[524288]>

Do you want to use adaptive rules to compute the threat level of messages? [Y]>

Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> Y

Logging of URLs has been enabled.
```

```
The Outbreak Filters feature is now globally enabled on the system.  You must use the
'policyconfig' command in the CLI or the Email

Security Manager in the GUI to enable Outbreak Filters for the desired Incoming and
Outgoing Mail Policies.

Choose the operation you want to perform:

- SETUP - Change Outbreak Filters settings.

[]>
```

アウトブレイク フィルタ ルール

アウトブレイク ルールは、Cisco Security Intelligence Operations から発行されます。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。このアップデート間隔を変更できます。詳細については、アップグレードおよびアップデートをダウンロードするためのサーバ設定を参照してください。

関連項目

- アウトブレイク フィルタ ルールの管理 （18 ページ）

アウトブレイク フィルタ ルールの管理

アウトブレイク フィルタ 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、何らかの理由でアプライアンスが一定期間シスコのアップデート サーバ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隔離しておく必要はありません。

[ルールを今すぐアップデート（Update Rules Now）] をクリックすることによって、シスコのアップデートサーバから、アップデートされたアウトブレイク ルールを手動でダウンロードできます。

（注） [ルールを今すぐアップデート（Update Rules Now）] ボタンは、アプライアンスの既存のアウトブレイク ルールを「フラッシュ」しません。アップデートされたアウトブレイク ルールを置き換えるだけです。シスコのアップデートサーバに利用可能なアップデートがない場合、アプライアンスはこのボタンをクリックするまでアウトブレイク ルールをダウンロードしません。

関連項目

- アウトブレイク フィルタ ルールのアップデート （19 ページ）

アウトブレイク フィルタ ルールのアップデート

デフォルトでは、アプライアンスは 5 分ごとに新しいアウトブレイク フィルタ ルールのダウンロードを試行します。この間隔は、[セキュリティサービス（Security Services）]>[サービスのアップデート（Service Updates）] ページで変更できます。詳細については、サービス アップデートを参照してください。

アウトブレイク フィルタ機能とメール ポリシー

アウトブレイク 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。アウトブレイク フィルタ機能は、アプライアンスでメール 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およびドメインをアウトブレイク フィルタ機能の処理から除外できます。この機能は、policyconfig CLI コマンドによっても使用可能です（『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』を参照）。

（注） アウトブレイク フィルタ機能が非ウイルス性の脅威をスキャンするために、Anti-Spam または Intelligent Multi-Scan スキャンをアプライアンスでグローバルにイネーブルにする必要があります。

特定のメール ポリシーに対するアウトブレイク 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 [アウトブレイクフィルタ（Outbreak Filters）] 列のリンクをクリックします。

特定のメール ポリシーに対してアウトブレイク フィルタ機能をイネーブルにし、カスタマイズするには、[アウトブレイクフィルタを有効にする（設定をカスタマイズ）（Enable Outbreak Filtering (Customize Settings)）] を選択します。

メール ポリシーに対して次のアウトブレイク フィルタ設定を構成できます。

- 隔離脅威レベル
- 最大隔離保持期間
- 非ウイルス性の脅威メッセージを隔離に追加せずに即時に配信
- バイパスするファイル拡張子のタイプ
- メッセージ変更のしきい値
- カスタム テキストおよびアウトブレイク フィルタ変数（$threat_verdict、$threat_category、$threat_type、$threat_description、および $threat_level など）を使用して件名ヘッダーを変更します。
- 次の電子メール ヘッダーを組み込みます。
  - X-IronPort-Outbreak-Status
  - X-IronPort-Outbreak-Description

- E メール セキュリティ アプライアンスまたは Exchange サーバなどの代替宛先にメッセージを送信します。
- URL 書き換え
- 脅威の免責事項

[アウトブレイクフィルタを有効にする（デフォルトのメールポリシー設定を継承）（Enable Outbreak Filtering (Inherit Default mail policy settings)）] を選択して、デフォルトのメール ポリシーについて定義されているアウトブレイク フィルタ設定を使用します。デフォルト メール ポリシーでアウトブレイク フィルタ機能をイネーブルにしている場合は、その他すべてのメール ポリシーはカスタマイズしない限り同じアウトブレイク フィルタ設定を使用します。

設定を変更したら、変更を確定します。

関連項目

- 隔離レベルのしきい値の設定 （20 ページ）
- 最大隔離保持 （20 ページ）
- ファイル拡張子タイプのバイパス （21 ページ）
- メッセージ変更 （21 ページ）

隔離レベルのしきい値の設定

リストからアウトブレイクの脅威に対する[隔離する脅威レベル（Quarantine Threat Level）]のしきい値を選択します。数字が小さいほど隔離されるメッセージは多くなり、数字が大きいほど隔離されるメッセージは少なくなります。シスコは、デフォルト値の 3 を推奨します。

詳細については、隔離脅威レベルのしきい値設定ガイドライン （9 ページ）を参照してください。

最大隔離保持

メッセージがアウトブレイク隔離エリアに留まる最大時間を指定します。ウイルス性の添付ファイルを含む可能性のあるメッセージ、およびフィッシングやマルウェア リンクなどその他の脅威を含む可能性のあるメッセージに対して異なる保持期間を指定できます。非ウィルス性の脅威の場合は、メッセージを隔離に追加せずに即時に配信するには [隔離に追加せずにメッセージを送信します（Deliver messages without adding them to quarantine）] チェックボックスをオンにします。

（注） ポリシーで[メッセージの変更（Message Modification）]をイネーブルにしない限り、非ウイルス性の脅威を隔離できません。

CASEは、メッセージに脅威レベルを割り当てるときに隔離保持期間を推奨しています。E メール セキュリティ アプライアンスは、脅威タイプに対する最大隔離保持期間を超えない限り、CASE が推奨する時間の長さの間、隔離されるメッセージを保持します。

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 によるメッセージの脅威レベル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 パイプライン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、[添付ファイルのスキャンのバイパス（Bypass Attachment Scanning）] をクリックし、ファイル拡張子を選択または入力してから、[拡張子を追加（Add Extension）] をクリックします。AsyncOS は、[バイパスするファイル拡張子（File Extensions to Bypass）] リストに拡張子タイプを表示します。

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、[バイパスするファイル拡張子（File Extensions to Bypass）] リストの拡張子の横のゴミ箱アイコンをクリックします。

関連項目

- ファイル拡張子のバイパス：コンテナ ファイルのタイプ （21 ページ）

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。

メッセージ変更

アプライアンスがフィッシングの試行またはマルウェア Web サイトへのリンクなど非ウイルス性の脅威のメッセージをスキャンする場合は、[メッセージの変更（Message Modification）] をイネーブルにします。

メッセージの脅威レベルに基づいて、AsyncOS はメッセージを変更し、すべての URL を書き換えて、メッセージから Web サイトを開こうとすると Cisco Web セキュリティ プロキシを経由して受信者をリダイレクトすることができます。アプライアンスはメッセージに免責事項を追加して、ユーザにメッセージの内容が疑わしい、または不正であることを警告することもできます。

非ウイルス性の脅威メッセージを隔離するために、メッセージ変更をイネーブルにする必要があります。

関連項目

- メッセージ変更の脅威レベル （22 ページ）
- メッセージの件名 （22 ページ）
- アウトブレイク フィルタの電子メール ヘッダー （22 ページ）
- 代替宛先メール ホスト （23 ページ）
- URL 書き換えおよびドメインのバイパス （23 ページ）
- 脅威の免責事項 （24 ページ）

メッセージ変更の脅威レベル

リストから [メッセージの変更 - 脅威レベル（Message Modification Threat Level）] のしきい値を選択します。この設定は、CASE によって返される脅威レベルに基づいて、メッセージを変更するかどうかを決定します。数字が小さいほど変更されるメッセージは多くなり、数字が大きいほど変更されるメッセージは少なくなります。シスコは、デフォルト値の 3 を推奨します。

メッセージの件名

変更されたリンクを含む非ウイルス性の脅威メッセージで件名ヘッダーのテキストを変更すると、ユーザにメッセージが保護のために変更されたことを通知できます。カスタムテキストとアウトブレイク フィルタ変数（`$threat_verdict`、`$threat_category`、`$threat_type`、`$threat_description`、および `$threat_level` など）のいずれかまたは両方を、件名ヘッダーの前または後に追加します。変数を挿入するには、[変数の挿入（Insert Variables）] をクリックし、変数のリストから選択します。

[メッセージの件名（Message Subject）] フィールドでは、空白は無視されません。このフィールドに入力したテキストの後ろまたは前にスペース追加することで、オリジナルのメッセージ件名と、追加テキストを分けることができます（追加テキストをオリジナルの件名の前に追加する場合は追加テキストの前、オリジナルの件名の後ろに追加する場合は追加テキストの後ろにスペースを追加します）。たとえば、`[MODIFIED FOR PROTECTION]` というテキストをオリジナルの件名の前に追加する場合は、この後ろに数個のスペースを追加します。

（注） [メッセージの件名（Message Subject）] フィールドでは、US-ASCII 文字だけを使用できます。

アウトブレイク フィルタの電子メール ヘッダー

次のヘッダーをメッセージに追加できます。

ヘッダー	フォーマット（Format）	例	オプション
X-IronPort-Outbreak-Status	`X-IronPort-Outbreak-Status: $threat_verdict, level $threat_level, $threat_category - $threat_type`	`X-IronPort-Outbreak-Status: Yes, level 4, Phish - Password`	• すべてのメッセージで有効（Enable for all messages） • 非ウイルス性アウトブレイクでのみ有効（Enable only for non-viral outbreak） • 無効（Disable）
X-IronPort-Outbreak-Description	`X-IronPort-Outbreak-Description: $threat_description`	`X-IronPort-Outbreak-Description: It may trick victims into submitting their username and password on a fake website.`	• 有効（Enable） • 無効

（注） これらのヘッダーに基づいてメッセージをフィルタリングする場合は、（代替宛先メール ホストを設定して）アウトブレイク フィルタで処理されたメッセージを E メール セキュリティ アプライアンスに戻し、これらのヘッダーに一致するコンテンツ フィルタを使用してメッセージをスキャンする必要があります。

代替宛先メール ホスト

アウトブレイク フィルタにより処理されたメッセージに対してコンテンツ フィルタ ベースのスキャンを実行する場合は、処理されたメッセージを E メール セキュリティ アプライアンスに戻すようにアウトブレイク フィルタを設定する必要があります。これは、処理パイプラインではコンテンツ フィルタ スキャンの後にアウトブレイク フィルタ スキャンが実行されるためです。

[代替宛先メールホスト（Alternate Destination Mail Host）] フィールドに、処理後のメッセージをさらにスキャンするために送信する送信先アプライアンスの IP アドレス（IP v 4 または IPv6）または FQDN を入力します。

URL 書き換えおよびドメインのバイパス

メッセージの脅威レベルがメッセージ変更のしきい値を超える場合、アウトブレイク フィルタ機能はメッセージ内のすべての URL を書き換え、これらの URL をクリックするとユーザを Cisco Web セキュリティ プロキシのスプラッシュ ページにリダイレクトします。（詳細については、URL のリダイレクト （5 ページ）を参照してください）。メッセージの脅威レベルが隔離のしきい値を超える場合、アプライアンスがメッセージの隔離も行います。小規模の非ウイルス性のアウトブレイクが進行中の場合、メッセージの隔離は TOC に、アウトブレイクの可能性があるメッセージからリンクされるすべての疑わしい Web サイトを分析し、その Web サイトが不正であるかどうか判断する時間を与えます。CASE は、SIO が提供するアップデートされたアウトブレイク ルールを使用してメッセージを再スキャンし、メッセージがアウトブレイクの一部であるかを判断します。保持期間が過ぎると、アプライアンスはメッセージを隔離エリアから解放します。

AsyncOS は、バイパスされるドメインを指している URL を除き、メッセージ内のすべての URL を書き換えます。

[URLの書き換え（URL Rewriting）] では次のオプションを使用できます。

- [未署名のメッセージでのみ有効（Enable only for unsigned messages）]：このオプションによって、AsyncOS は、メッセージ変更のしきい値を満たすか超える未署名のメッセージ内の URL を書き換えられるようになります。ただし、署名されたメッセージは含まれません。URL 書き換えについて、シスコはこの設定の使用を推奨します。

（注） E メール セキュリティ アプライアンス以外のネットワーク上のサーバまたはアプライアンスが DomainKeys/DKIM 署名の検証を担当する場合、E メール セキュリティ アプライアンスは、DomainKeys/DKIM-signed メッセージ内の URL を書き換えたり、メッセージの署名を無効にしたりすることができます。

S/MIME を使用して暗号化されている場合または S/MIME 署名が含まれる場合、アプライアンスはメッセージを署名済みとみなします。

- **[すべてのメッセージで有効（Enable for all messages）]**：このオプションによって、AsyncOS は、メッセージ変更のしきい値を満たすか超えるすべてのメッセージ内の URL を書き換えられるようになります。署名されたメッセージも含まれます。AsyncOS が署名されたメッセージを変更すると、署名は無効になります。
- **[無効（Disable）]**：このオプションはアウトブレイク フィルタに対して URL 書き換えをディセーブルにします。

ポリシーを変更して、特定のドメインへの URL を変更から除外できます。ドメインをバイパスするには、IPv4 アドレス、IPv6 アドレス、CIDR 範囲、ホスト名、部分ホスト名、またはドメインを [ドメインのスキャンをバイパス（Bypass Domain Scanning）] フィールドに入力します。複数のエントリを指定する場合は、カンマで区切ります。

バイパス ドメイン スキャン機能は、URL フィルタリングで使用されるグローバル ホワイトリストに似ていますが、このホワイトリストとは関係ありません。ホワイトリストの詳細については、URL フィルタリングのホワイトリストの作成を参照してください。

脅威の免責事項

E メール セキュリティ アプライアンスは、疑わしいメッセージのヘッダーの上部に免責事項メッセージを追加して、ユーザにメッセージの内容を警告することができます。この免責事項には、メッセージのタイプに応じて HTML またはプレーン テキストが使用できます。

[脅威に関する免責事項（Threat Disclaimer）] リストから使用する免責事項のテキストを選択するか、[メールポリシー（Mail Policies）] > [テキストリソース（Text Resources）] リンクをクリックし、[免責事項テンプレート（Disclaimer Template）] を使用して新しい免責事項を作成します。[免責事項テンプレート（Disclaimer Template）] には、アウトブレイク脅威情報に関する変数が含まれます。[免責事項のプレビュー（Preview Disclaimer）] をクリックすると、脅威免責事項のプレビューを表示できます。カスタム免責事項メッセージでは、変数を使用してメッセージの脅威レベル、脅威のタイプ、および脅威の説明を表示できます。免責事項メッセージの作成については、テキスト リソース管理の概要を参照してください。

アウトブレイク フィルタ機能とアウトブレイク隔離

アウトブレイク フィルタ機能により隔離されたメッセージは、アウトブレイク隔離エリアに送信されます。この隔離エリアは、メッセージを隔離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、隔離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、その他のあらゆる隔離と同様に機能します（隔離の操作方法の詳細については、ポリシー、ウイルス、およびアウトブレイク隔離を参照してください）。サマリー ビューの詳細については、[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 （26 ページ）を参照してください。

関連項目

- アウトブレイク隔離のモニタリング （25 ページ）
- [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 （26 ページ）

アウトブレイク隔離のモニタリング

適切に設定された隔離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、アウトブレイク隔離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隔離された場合、アウトブレイク隔離の設定によっては、次のいずれかが発生します。

- 隔離のデフォルト アクションが [リリース（Release）] に設定されている場合は、保持期間の期限が切れたとき、または隔離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、アウトブレイク隔離を設定できます。これらのアクションの詳細については、隔離メッセージに自動的に適用されるデフォルト アクションを参照してください。
- 隔離のデフォルト アクションが [削除（Delete）] に設定されている場合は、保持期間の期限が切れたとき、または隔離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、隔離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、アウトブレイク隔離を設定できます。

隔離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、アウトブレイク隔離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（Delete）] に設定されている場合は、アウトブレイク隔離エリアをモニタすることが重要です。シスコは、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（Delete）] に設定しないことを推奨します。アウトブレイク隔離エリアからのメッセージの解放、またはアウトブレイク隔離のデフォルト アクションの変更に関する

詳細については、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を参照してください。

反対に、新しいルールのアップデートを待つ間、アウトブレイク隔離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、隔離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。

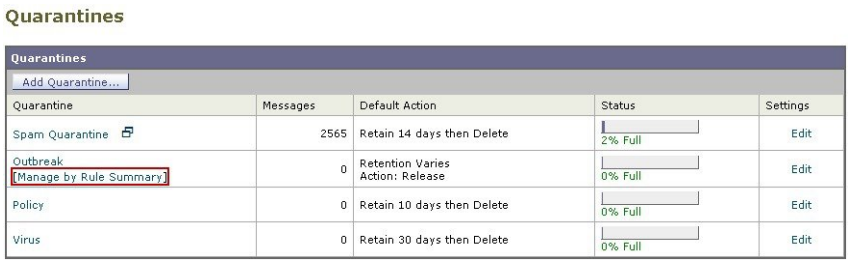
（注） メッセージがアウトブレイク隔離エリアに留まっている間にアンチウイルス スキャンが（メールポリシーごとではなく）グローバルにディセーブルにされた場合は、たとえメッセージが解放される前にもう一度アンチウイルス スキャンを再度イネーブルにしたとしても、そのメッセージが解放されたときのアンチウイルス スキャンは実行されません。

（注） アウトブレイク フィルタ機能は、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。ただし、アプライアンスでアンチスパム スキャンがイネーブルでない場合は、アウトブレイク フィルタは非ウイルス性の脅威をスキャンできません。

[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

GUI の [モニタ（Monitor）] メニューにあるリスト内の隔離名をクリックすることで、アウトブレイク隔離エリアの内容を表示できます。アウトブレイク隔離には、追加のビューである、アウトブレイク隔離の [ルールサマリーによる管理（Manage by Rule Summary）] リンクもあります。

図 *3:* アウトブレイク隔離の *[ルールサマリーによる管理（Manage by Rule Summary）]* リンク



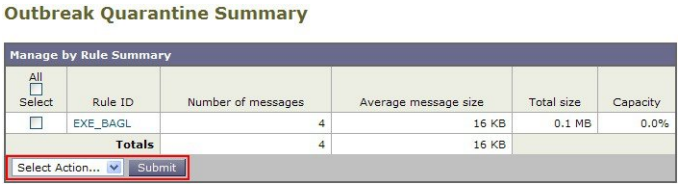
関連項目

- サマリー ビューの使用によるアウトブレイク隔離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 （27 ページ）

サマリー ビューの使用によるアウトブレイク隔離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

[ルールサマリーによる管理（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アウトブレイク隔離の内容のリストを表示します。

図 4 : アウトブレイク隔離の *[ルールサマリーによる管理（Manage by Rule Summary）]* ビュー



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 -> outbreakmanage CLI コマンドからも使用できます。詳細については、『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』を参照してください。

アウトブレイク フィルタのモニタリング

アプライアンスには、アウトブレイク 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複数のツールが含まれています。

関連項目

- アウトブレイク フィルタ レポート （27 ページ）
- アウトブレイク フィルタの概要とルール リスト （28 ページ）
- アウトブレイク隔離 （28 ページ）
- アラート、SNMP トラップ、およびアウトブレイク フィルタ （28 ページ）

アウトブレイク フィルタ レポート

アプライアンスのアウトブレイク フィルタの現在のステータスおよび設定に加えて、最近のアウトブレイクやアウトブレイク フィルタによって隔離されたメッセージに関する情報が表示されるアウトブレイク フィルタ レポートです。この情報は、[モニタ（Monitor）] > [アウトブレイクフィルタ（Outbreak Filters）] ページで表示します。詳細については、「電子メール セキュリティ モニタ」の章を参照してください。

アウトブレイク 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、アウトブレイク 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、[セキュリティサービス（Security Services）] > [アウトブレイク フィルタ（Outbreak Filters）] ページで表示します。

アウトブレイク隔離

アウトブレイク隔離を使用して、アウトブレイク 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メッセージの数をモニタします。また、ルールごとの隔離メッセージのリストも使用できます。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 （26 ページ）およびポリシー、ウイルス、およびアウトブレイク隔離を参照してください。

アラート、SNMP トラップ、およびアウトブレイク フィルタ

アウトブレイク 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、「CLI を使用した管理とモニタ」の章を参照してください。

AsyncOS のアウトブレイク 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、アウトブレイク隔離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、隔離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。隔離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。

アウトブレイクフィルタ機能のトラブルシューティング

この項では、アウトブレイク 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。

関連項目

- 誤って分類されたメッセージのシスコへの報告 （29 ページ）
- 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 （29 ページ）
- 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 （29 ページ）

誤って分類されたメッセージのシスコへの報告

[隔離の管理（Manage Quarantine）] ページのチェックボックスを使用すると、アウトブレイク隔離がシスコに対して誤分類を通知するようになります。

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、アウトブレイク 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、メッセージがアウトブレイク 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。