ゾーンのフィルタの設定

この章では、高度なゾーンのフィルタの設定作業を実施する方法について説明します。WBM を使用すると、ゾーンのトラフィックを処理するためのカスタムフィルタ設定を設計できます。

この章は、次の項で構成されています。

ゾーンのフィルタの概要

Detector モジュールは、ゾーン フィルタを使用して、Detector モジュールが受信するトラフィック フローのコピーを管理します。ゾーン フィルタは Detector モジュールをイネーブルにして、次の機能を実行します。

- ゾーンのトラフィックに異常がないかどうかを分析する。
- Detector モジュールが異常を検出した場合、通知を送信するか、Cisco Anomaly Guard Module をアクティブにする。
- すぐにトラフィックをドロップし、Detector モジュールの異常検出機能をバイパスする。

トラフィックの管理および DDoS 攻撃の検出用のゾーン固有の規則を Detector モジュールに提供するゾーン フィルタのセットを設定できます。ゾーンのフィルタの設定を変更すると、変更した内容がただちに有効になります。Detector モジュールは、次のタイプのトラフィック フィルタを使用します。

- ユーザ フィルタ : Detector モジュールには、静的なユーザ フィルタのセットがあらかじめ設定されています。このユーザ フィルタは、ユーザが GUARD ゾーン テンプレートを使用して作成するゾーンに対して適用されます。ユーザ フィルタは、Cisco Anomaly Guard Module でのみ使用され、トラフィック フローに特定の保護レベルを適用します。ユーザ フィルタは、さまざまなタイプの攻撃に対応するように設計されています。

  Cisco Anomaly Guard Module は、ユーザ フィルタと動的フィルタ（下記の説明を参照）の両方を利用して、攻撃の進行中にゾーン保護を管理します。ゾーンに対する攻撃が発生すると、Cisco Anomaly Guard Module は、攻撃の進行中に保護プロセスを管理するアクションを設定する動的フィルタの作成を開始します。Cisco Anomaly Guard Module は、十分な時間を費やして攻撃を分析するまでの間、ユーザ フィルタにトラフィック フローを誘導するアクションを実行する動的フィルタを設定します。ユーザ フィルタは、攻撃に対する最初の防御手段となって、ユーザ フィルタが持つアクションをトラフィックに適用します。Cisco Anomaly Guard Module は攻撃の分析を終えると、トラフィック フローに直接適用する独自のアクションを実行する動的フィルタの作成を開始します。Cisco Anomaly Guard Module がトラフィック フローにユーザ フィルタと動的フィルタの両方の適用を試みる場合、より厳しいアクションを実行するフィルタが選択されます。

- 動的フィルタ：（Detector モジュールの動作）Detector モジュールは、攻撃進行中のトラフィック フローの分析結果として動的フィルタを作成します。動的フィルタは、Detector モジュールが Detector モジュールの syslog にイベントを記録するか、Guard をアクティブにしてゾーンを保護するように誘導します。

  （Cisco Anomaly Guard Module の動作）Cisco Anomaly Guard Module は、攻撃進行中のトラフィック フローの分析結果として動的フィルタを作成します。ユーザ フィルタと同様に、動的フィルタも特定の保護レベルをトラフィック フローに適用します。Cisco Anomaly Guard Module は、動的フィルタをゾーンのトラフィックおよび特定の DDoS 攻撃に合せて継続的に調整します。動的フィルタは有効期間が限定されており、攻撃が終了すると Cisco Anomaly Guard Module によって削除されます。動的フィルタは、ユーザが追加または削除できます。

- バイパス フィルタ：ユーザ定義のバイパス フィルタを使用すると、特定のトラフィック フローを Detector が処理しなくなります。バイパス フィルタを追加することで、トラフィックに異常がないかどうかを Detector が分析する前にトラフィック フローのコピーをドロップできます。

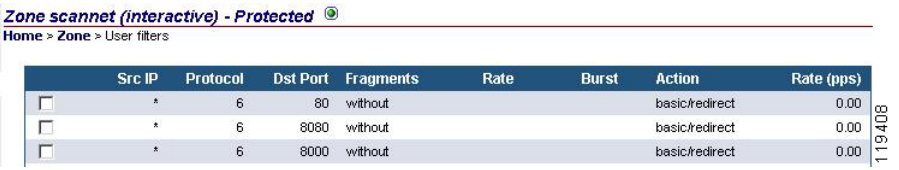
- フレックスコンテンツ フィルタ：ユーザ定義のフレックスコンテンツ フィルタを使用すると、Detector モジュールで指定のパケット フローのパケットをカウントしたり、悪意のあるトラフィックの送信元を特定したりできます。このバークリー パケット フィルタは、IP ヘッダーおよび TCP ヘッダーのフィールドに基づいたフィルタリングや、コンテンツのバイト数に基づいたフィルタリングなど、柔軟なフィルタリング機能を提供します。フレックスコンテンツ フィルタは、特定のトラフィック フローに対して設定します。設定できるフレックスコンテンツ フィルタは、ゾーンごとに 1 つのみです。フレックスコンテンツ フィルタはリソース消費量が多く、パフォーマンスに影響を及ぼす可能性があるため、十分に注意して使用してください。

  バークリー パケット フィルタの設定オプションの詳細については、http://www.freesoft.org/CIE/Topics/56.htm を参照してください。

ユーザ フィルタの管理

次の手順では、GUARD ゾーン テンプレートを使用して作成するゾーン設定にユーザ フィルタを追加する方法、またはそのゾーン設定からユーザ フィルタを削除する方法について説明します（ユーザ フィルタは、Cisco Anomaly Guard Module でのみ使用されます）。Cisco Anomaly Guard Module は、ユーザ フィルタ リストに表示される順序でユーザ フィルタをアクティブにします（図 5-1 を参照）。新しいユーザ フィルタを追加するときは、リスト内での新しいフィルタの配置場所を把握しておくことが重要です。

図 5-1　　ユーザ フィルタ



この項では、次の手順について説明します。

- ユーザ フィルタの追加
- ユーザ フィルタの削除

ユーザ フィルタの追加

新しいユーザ フィルタを追加するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインで、GUARD ゾーン テンプレートを使用して作成したゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > User filters** を選択します。ゾーンのユーザ フィルタのリストが表示されます（図 5-1 を参照）。

ステップ 3　**Add** をクリックします。Add Filter Step 1 画面が表示され、ユーザ フィルタのリストが示されます。

ステップ 4　Insert カラムで、ユーザ フィルタを挿入する位置の下にある行をクリックします。Insert Here テキストが表示され、選択した行の上に新しいユーザ フィルタが挿入されることが示されます。

ステップ 5　**Next** をクリックします。Add Filter Step 2 画面が表示され、User Filter Form が示されます。

ステップ 6　新しいユーザ フィルタのパラメータを設定します。表 5-1 に、User Filter Form に表示されるフィルタ パラメータの説明を示します。

表 5-1　ユーザ フィルタのパラメータ

パラメータ	説明
Source IP	特定の IP アドレスから送信されるトラフィックをユーザ フィルタに転送します。送信元 IP アドレスを入力します。すべての送信元 IP アドレスを指定するには、このフィールドをブランクのままにするか、アスタリスク（*）を入力します。
Source subnet	特定のサブネットから送信されるトラフィックをユーザ フィルタに転送します。サブネットを Source subnet ドロップダウン リストから選択します。
Protocol	特定のプロトコルで送信されるトラフィックをユーザ フィルタに転送します。プロトコル番号を入力します。すべてのプロトコルを指定するには、このフィールドをブランクのままにするか、アスタリスク（*）を入力します。
Dst Port	特定のポートが宛先となっているトラフィックをユーザ フィルタに転送します。宛先ポート番号を入力します。すべての宛先ポートを指定するには、このフィールドをブランクのままにするか、アスタリスク（*）を入力します。

表 5-1　ユーザ フィルタのパラメータ（続き）

パラメータ	説明
Fragments	フィルタで処理するトラフィックのタイプを指定します。Fragments ドロップダウン リストから、次のいずれかを選択します。 • **without**：ユーザ　フィルタは断片化されていないトラフィックを処理します。 • **with**：ユーザ フィルタは断片化されたトラフィックを処理します。 • *****：ユーザ フィルタは、断片化されたトラフィックと断片化されていないトラフィックの両方を処理します。
Rate	レート リミットを指定します。ユーザ フィルタは、トラフィックの量を指定したレート以下に制限します。レート リミットの値を Rate フィールドに入力し、使用する測定単位を Rate ドロップダウン リストから選択します。トラフィック レートをユーザ フィルタで制限しない場合は、測定単位として **unlimit** を選択します。
Burst	トラフィックのバースト リミットを指定します。ユーザ フィルタは、Rate に対して選択したものと同じ測定単位をバーストにも使用します（このテーブルの Rate を参照）。
Action	特定のトラフィック タイプに対してユーザ フィルタが実行するアクションを指定します。Action ドロップダウン リストから、次のいずれかを選択します。 • **permit**：フローの統計分析を実行せず、このフローをスプーフィング防止保護メカニズムとゾンビ防止保護メカニズムによって処理しない場合に使用します。このフローは他の保護メカニズムによって処理されないため、このフィルタにはレート リミットとバースト リミットを設定することをお勧めします。 • **basic/redicrect**：HTTP 経由のアプリケーションを認証する場合に使用します。 • **basic/reset**：TCP 経由のアプリケーションを認証する場合に使用します。HTTP トラフィック フローには basic/redirect アクションを使用することをお勧めします。

表 5-1　ユーザ フィルタのパラメータ（続き）

パラメータ	説明
Action （続き）	• **basic/safe-reset**：TCP 接続のリセットを許容しない TCP アプリケーション トラフィック フローを認証する場合に使用します。HTTP トラフィック フローには basic/redirect アクションを使用することをお勧めします。 • **basic/default**：TCP 以外のトラフィック フローを認証する場合に使用します。 • **basic/dns-proxy**：TCP DNS トラフィック フローを認証する場合に使用します。 • **strong**：トラフィック フローの強化認証が必要な場合や、それまでのフィルタが該当するアプリケーションに適していないと考えられる場合に使用します。認証は、各接続に対して行われます。 TCP 着信接続には Detector モジュールがプロキシの役割を果たすため、このような接続に対するこのアクションは、ACL（アクセス コントロール リスト）を使用しているなど、ネットワークが IP アドレスに従って管理される場合には使用しないことをお勧めします。 • **drop**：トラフィック フローをドロップする場合に使用します。

ステップ 7　次のいずれかのオプションを選択します。

- **OK**：新しいユーザ フィルタの設定を保存します。User filters 画面が表示されます。
- **Cancel**：情報を保存せずに User Filters Form を終了します。User filters 画面が表示されます。

ユーザ フィルタの削除

注意　Cisco Anomaly Guard Module のゾーン保護の機能に影響を及ぼす可能性があるので、ユーザ フィルタを削除する場合は、注意してください。

ユーザ フィルタを削除するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインで、GUARD ゾーン テンプレートを使用して作成したゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > User filters** を選択します。ゾーンのユーザ フィルタのリストが表示されます。

ステップ 3　削除するユーザ フィルタの隣にあるチェックボックスをオンにします。

ステップ 4　**Delete** をクリックします。ユーザ フィルタのリストからユーザ フィルタが削除されます。

バイパス フィルタの管理

次の手順では、Detector モジュールのバイパス フィルタを追加または削除する方法について説明します。ここに示す手順に従ってバイパス フィルタのリストを表示すると、バイパス フィルタでフィルタリングされた現在のバイパス フィルタ トラフィックのレートが、カウンタにパケット / 秒（pps）単位で示されます。

この項では、次の手順について説明します。

- バイパス フィルタの追加
- バイパス フィルタの削除

バイパス フィルタの追加

バイパス フィルタを追加するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > Bypass filters** を選択します。Bypass filters 画面が表示されます。

ステップ 3　**Add** をクリックします。Add bypass filter 画面が表示されます。

ステップ 4　新しいバイパス フィルタのパラメータを設定します。表 5-2 に、Bypass Filter Form に表示されるフィルタ パラメータの説明を示します。

表 5-2　バイパス フィルタのパラメータ

パラメータ	説明
Source IP	Detector モジュールは、ユーザが指定する IP アドレスからのトラフィックを直接ゾーンに転送し、Detector モジュールの異常検出機能をバイパスします。すべての送信元 IP アドレスを指定するには、このフィールドをブランクのままにするか、アスタリスク（*）を入力します。

表 5-2　バイパス フィルタのパラメータ（続き）

パラメータ	説明
Source subnet	Detector モジュールは、ユーザが指定するサブネットからのトラフィックを直接ゾーンに転送し、Detector モジュールの異常検出機能をバイパスします。サブネットを Source subnet ドロップダウン リストから選択します。
Protocol	Detector モジュールは、ユーザが指定するプロトコルを使用してトラフィックを直接ゾーンに転送し、Detector モジュールの異常検出機能をバイパスします。プロトコル番号を入力します。すべてのプロトコルを指定するには、このフィールドをブランクのままにするか、アスタリスク（*****）を入力します。
Dst Port	Detector モジュールは、ユーザが指定するゾーンの宛先ポートをターゲットとするトラフィックを転送し、Detector モジュールの異常検出機能をバイパスします。宛先ポート番号を入力します。すべての宛先ポートを指定するには、このフィールドをブランクのままにするか、アスタリスク（*****）を入力します。
Fragments	フィルタで処理するトラフィックのタイプを指定します。Fragments ドロップダウン リストから、次のいずれかを選択します。 • **without**：バイパス フィルタは断片化されていないトラフィックを処理します。 • **with**：バイパス　フィルタは断片化されたトラフィックを処理します。 • *****：バイパス フィルタは、断片化されたトラフィックと断片化されていないトラフィックの両方を処理します。

ステップ 5　次のいずれかのオプションを選択します。

- **OK**：新しいバイパス フィルタの設定を保存します。Bypass filters 画面が表示されます。
- **Cancel**：情報を保存せずに Bypass Filters Form を終了します。Bypass filters 画面が表示されます。

バイパス フィルタの削除

バイパス フィルタを削除するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > Bypass filters** を選択します。Bypass filters 画面が表示されます。

ステップ 3　削除する各バイパス フィルタの隣にあるチェックボックスをオンにし、**Delete** をクリックします。フィルタのリストからバイパス フィルタが削除されます。表示されているバイパス フィルタをすべて削除するには、Src IP の隣にあるチェックボックスをオンにし、**Delete** をクリックします。

フレックスコンテンツ フィルタの管理

フレックスコンテンツ フィルタを使用すると、パケット ヘッダーのフィールドまたはパケット ペイロードのパターンに基づいて、ゾーンのトラフィックをフィルタリングできます。着信トラフィックに現れているパターンに基づいて攻撃を識別できます。このようなパターンによって、一定のパターンを持つ既知のワームやフラッド攻撃を識別できます。ただし、フレックスコンテンツ フィルタはリソースを大量に消費します。フレックスコンテンツ フィルタの使用はパフォーマンスに影響を与える場合があるため、注意してください。特定のポートに送信される TCP トラフィックなど、動的フィルタによって識別できる特定の攻撃からの保護にフレックスコンテンツ フィルタを使用する場合は、動的フィルタを使用してトラフィックをフィルタリングすることをお勧めします。

フレックスコンテンツ フィルタは、豊富なフィルタリング機能を持つバークリー パケット フィルタとパターン フィルタを組み合せたものです。フレックスコンテンツ フィルタは、目的のパケット フローをカウントし、トラフィックの特定の悪意ある送信元を明らかにするために使用します。

フレックスコンテンツ フィルタは、次の順序でフィルタリング基準を適用します。

1. プロトコルと宛先ポートに基づいて、パケットをフィルタリングします。
2. tcpdump 式を適用します。
3. 残ったパケットに対して、パターンを使用してパターン　マッチングを実行します。

この項は、次の情報と手順で構成されています。

- フレックスコンテンツ フィルタの式の構文について
- フレックスコンテンツ フィルタのパターンの構文について
- フレックスコンテンツ フィルタの追加
- フレックスコンテンツ フィルタの削除

フレックスコンテンツ フィルタの式の構文について

フレックスコンテンツ フィルタの式には、パケットとのパターン マッチングに使用する式を指定します。この式は、バークリー パケット フィルタ形式を使用して定義します。

（注）　宛先ポートとプロトコルに基づいてトラフィックをフィルタリングする場合は、tcpdump の式を使用できます。ただし、パフォーマンスを考慮すると、これらの基準に基づいてトラフィックをフィルタリングする場合は、フレックスコンテンツ フィルタの protocol パラメータと port パラメータを使用することをお勧めします。

表 5-3 に、フレックスコンテンツ フィルタの式のパラメータの説明を示します。

表 5-3　フレックスコンテンツ フィルタの式のパラメータ

パラメータ	説明
Destination host IP address	宛先ホスト IP アドレスへのトラフィック。
Source host IP address	送信元ホスト IP アドレスからのトラフィック。
Host IP address	送信元および宛先の両方のホスト IP アドレスの間のトラフィック。
Net mask	特定のネットワークへのトラフィック。
Net net/len	特定のサブネットへのトラフィック。
Destination port number	宛先ポート番号への TCP または UDP トラフィック。
Source port number	送信元ポート番号からの TCP または UDP トラフィック。
Port number	送信元および宛先の両方のポート番号間の TCP または UDP トラフィック。
Less packet length	特定のバイト長以下の長さを持つパケット。
Greater packet length	特定のバイト長以上の長さを持つパケット。
IP protocol	ICMP、UDP、または TCP のプロトコル番号を持つパケット。
IP broadcast	ブロードキャスト IP パケット。
IP multicast	マルチキャスト パケット。

表 5-3　フレックスコンテンツ フィルタの式のパラメータ（続き）

パラメータ	説明
Ether protocol	IP、ARP、または RARP などの特定のプロトコル番号またはプロトコル名を持つイーサネット プロトコル パケット。
Relop expression	特定の式に適合するトラフィック。詳細については、表 5-4 を参照してください。

表 5-4 に、フレックスコンテンツ フィルタの式の規則の説明を示します。

表 5-4　フレックスコンテンツ フィルタの式の規則

式の規則	
relop	>、<、>=、<=、=、!=
expression	整数の定数（標準の C 構文で表現されたもの）、通常のバイナリ演算子（+、-、*、/、&、|）、長さ演算子、および特殊なパケット データ アクセスで構成される算術式。パケット内のデータにアクセスするには、次の構文を使用します。 *protocol* [*expression*: *size*]
protocol	インデックス操作用のプロトコル層を指定します。指定可能な値は、**ether**、**ip**、**tcp**、**udp**、または **icmp** です。指定されたプロトコル層までの相対的なバイト オフセットは、*expression* で指定されます。*size* パラメータはオプションです。目的のフィールドのバイト数を示し、1、2、または 4 になります。デフォルトは 1 です。*length* パラメータには、パケットの長さを指定します。

次の方法により、プリミティブを組み合せることができます。

- プリミティブとオペレータを小カッコで囲んだグループ（小カッコはシェルの特殊文字であるため、エスケープする必要があります）。
- 否定：**!** または **not** を使用します。
- 連結：**&&** または **and** を使用します。
- 代替：|| または **or** を使用します。

否定は、最も高い優先度を持ちます。代替と連結の優先順位は同じで、左から右に関連付けられます。連結には、並置ではなく、明示的な **and** トークンが必要です。キーワードなしで識別子を指定した場合は、最後に指定されたキーワードが使用されます。

バークリー パケット フィルタの設定オプションの詳細については、http://www.freesoft.org/CIE/Topics/56.htm を参照してください。

次の例は、断片化されていないデータグラムと断片化されたデータグラムのフラグメント 0 のみをカウントする方法を示しています。このフィルタは、TCP と UDP のインデックス操作に暗黙的に適用されます。たとえば、tcp[0] は常に TCP ヘッダーの最初のバイトを意味し、中間のフラグメントの最初のバイトを意味することはありません。

```
ip[6:2]&0x1fff=0
```

次の例は、すべての TCP RST パケットをカウントする方法を示しています。

```
tcp[13]&4!=0
```

次の例は、エコー要求およびエコー応答（ping）ではないすべての ICMP パケットをカウントする方法を示しています。

```
"icmp [0]!=8 and icmp[0] != 0"
```

次の例は、ポート 80 を宛先とし、ポート 1000 を送信元としないすべての TCP パケットをカウントする方法を示しています。

```
"tcp and dst port 80 and not src port 1000"
```

フレックスコンテンツ フィルタのパターンの構文について

パターン（正規表現）は、一連の文字を含んだ文字列を記述したものです。パターンには、パターンの要素を実際に列挙するのではなく、一連の文字列を記述します。パターンは、一般文字と特殊文字で構成されます。一般文字には、特殊文字とは見なされない印刷可能な ASCII 文字が含まれます。特殊文字は、どのようなマッチングを実行するのかを示します。フレックスコンテンツ フィルタは、このパターンをパケットの内容（パケットのペイロード）と照合します。たとえば、*version 3.1*、*version 4.0*、および *version 5.2* の 3 つの文字列は、*version* .*\..* というパターンで記述されます。

特殊文字とは、特殊な意味を持ち、Detector モジュールが式でどのようなマッチングを実行するかを示す文字です。表 5-5 に、ユーザが使用できる特殊文字の説明を示します。

表 5-5　フレックスコンテンツ パターン フィールドの説明

特殊文字	説明
.*	0 個またはそれ以上の文字を含んでいる文字列と一致します。たとえば、パターン *goo.*s* は *goos*、*goods*、*good for ddos* などと一致します。
\	特殊文字が持つ特殊な意味を取り除きます。特殊文字を文字列の中で 1 つの文字パターンとして使用するには、各文字の先頭にバックスラッシュ（\）を入力して特殊な意味を取り除きます。たとえば、シーケンス「\\」は「\」に、シーケンス「\.」は「.」に一致します。 文字として使用するアスタリスク（*）の前にもバックスラッシュを配置する必要があります。
\xHH	16 進値と一致します。H は 16 進数の数字で、大文字と小文字は区別されません。16 進値は 2 桁で入力する必要があります。たとえば、「\x41」は「A」と一致します。

次の例は、パケットのペイロードに特定のパターンが含まれているパケットをドロップする方法を示しています。この例のパターンは、Slammer ワームから抽出されたものです。プロトコル、ポート、および tcpdump 式は特定のものでなくてもかまいません。

```
\x89\xE5Qh\.dllhel32hkernQhounthickChGetTf\xB9ll
Qh32\.dhws2_f\xB9etQhsockf\xB9toQhsend\xBE\x18\x10\xAEB
```

フレックスコンテンツ フィルタの追加

フレックスコンテンツ フィルタを追加するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > Flex-Content filters** を選択します。Flex-Content filters 画面が表示され、既存のフレックスコンテンツ フィルタのリストが示されます。

ステップ 3　GUARD ゾーン テンプレートを使用してゾーンを作成した場合は、フレックスコンテンツ フィルタのリストの上に **View Detector/View Guard** トグル ボタンが表示されます。使用するフレックスコンテンツ フィルタ ビューを選択します。

- Detector モジュールが使用するフレックスコンテンツ フィルタを追加するには、**View Detector** をクリックします。
- Cisco Anomaly Guard Module が使用するフレックスコンテンツ フィルタを追加するには、**View Guard** をクリックします。

ステップ 4　**Add** をクリックします。Add filter - step 2 画面が表示されます。

ステップ 5　フレックスコンテンツ フィルタのパラメータを設定します。表 5-6 に、Flex-Content Filter Form に表示されるフィルタ パラメータの説明を示します。

表 5-6　フレックスコンテンツ フィルタのパラメータ

パラメータ	説明
Description	フレックスコンテンツ フィルタを説明するテキスト。
Protocol	特定のプロトコルを使用しているトラフィックを処理します。0 ～ 255 のプロトコル番号を入力します。すべてのプロトコル タイプを指定するには、アスタリスク（*）を入力します。 有効なプロトコル番号のリストについては、次の Internet Assigned Numbers Authority（IANA）の Web サイトを参照してください。 http://www.iana.org/assignments/protocol-numbers

表 5-6　フレックスコンテンツ フィルタのパラメータ（続き）

パラメータ	説明
Dst Port	特定の宛先ポートに向かうトラフィックを処理します。0 ～ 65535 の宛先ポート番号を入力します。すべての宛先ポートを指定するには、アスタリスク（*）を入力します。 有効なポート番号のリストについては、次の Internet Assigned Numbers Authority（IANA）の Web サイトを参照してください。 http://www.iana.org/assignments/port-numbers
Expression	指定した式に基づいてトラフィックをフィルタリングします（「フレックスコンテンツ フィルタの式の構文について」の項を参照）。180 個（スペース区切り）までのトークンを使用して文字列を入力します。
Pattern	パケットの内容と照合するための正規表現データ パターンを指定します（「フレックスコンテンツ フィルタのパターンの構文について」の項を参照）。使用するデータ パターンを入力します。
Match Case	データ パターン式で大文字と小文字を区別するかどうかを指定します。大文字と小文字を区別するデータ パターン式として定義するには、チェックボックスをオンにします。
Start Offset	パケットの内容の先頭から、パターン マッチングを開始する位置までのオフセットを指定します（バイト単位）。デフォルトは 0（ペイロードの先頭）です。開始オフセットは、pattern フィールドに適用されます。0 ～ 2047 の整数を入力します。
End Offset	パケットの内容の先頭から、パターン マッチングを終了する位置までのオフセットを指定します（バイト単位）。デフォルトは、パケット長（ペイロードの末尾）です。終了オフセットは、pattern フィールドに適用されます。0 ～ 2047 の整数を入力します。

表 5-6　フレックスコンテンツ フィルタのパラメータ（続き）

パラメータ	説明
Action	トラフィックに対してフレックスコンテンツ フィルタが実行するアクションを指定します。 アクションを Action ドロップダウン リストから選択します。 • **count**：フィルタに一致するトラフィック フロー パケットをカウントします。 • **drop**：フィルタに一致するトラフィック フロー パケットをドロップします。
State	フレックスコンテンツ フィルタの動作状態。 動作状態を State ドロップダウン リストから選択します。 • **enable**：Detector モジュールはフィルタをトラフィック フローに適用し、一致が検出されると設定されたアクションを実行します。 • **disable**：Detector モジュールは、フィルタをトラフィック フローに適用しません。

ステップ 6　次のいずれかのオプションを選択します。

- **OK**：新しいフレックスコンテンツ フィルタを保存します。Flex-Content filters 画面が表示されます。
- **Clear**：フォームの情報をデフォルト値に戻し、追加した情報をすべて消去します。
- **Cancel**：情報を保存せずに Flex-Content filters 画面を終了します。Flex-Content filters 画面が表示されます。

フレックスコンテンツ フィルタの削除

フレックスコンテンツ フィルタを削除するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > Flex-Content filters** を選択します。Flex-Content filters 画面が表示され、既存のフレックスコンテンツ フィルタのリストが示されます。

ステップ 3　GUARD ゾーン テンプレートを使用してゾーンを作成した場合は、フレックスコンテンツ フィルタのリストの上に **View Detector/View Guard** トグル ボタンが表示されます。

使用するフレックスコンテンツ フィルタ ビューを選択します。

- Detector モジュールが使用するフレックスコンテンツ フィルタを削除するには、**View Detector** をクリックします。
- Cisco Anomaly Guard Module が使用するフレックスコンテンツ フィルタを削除するには、**View Guard** をクリックします。

ステップ 4　削除する各フレックスコンテンツ　フィルタの隣にあるチェックボックスをオンにし、**Delete** をクリックします。フィルタのリストからフレックスコンテンツ フィルタが削除されます。表示されているフレックスコンテンツ フィルタをすべて削除するには、Src IP の隣にあるチェックボックスをオンにし、**Delete** をクリックします。