侵入ポリシー内のルールの管理

侵入ポリシーの [Rules] ページを使用して、共有オブジェクト ルール、標準テキスト ルール、およびプリプロセッサ ルールに関するルール状態とその他の設定を構成できます。

ルールは、ルール状態を [Generate Events] または [Drop and Generate Events] に設定することによって有効にします。ルールを有効にすると、システムがそのルールと一致するトラフィックに対するイベントを生成します。ルールを無効にすると、ルールの処理が停止されます。オプションで、インライン展開で [Drop and Generate Events] に設定されたルールによって、一致するトラフィックに対するイベントが生成され、そのトラフィックが破棄されるように、侵入ポリシーを設定できます。詳細については、「インライン展開での破棄動作の設定」（P.20-15）を参照してください。パッシブ展開では、[Drop and Generate Events] に設定されたルールによって、一致するトラフィックに対するイベントが生成されるだけです。

ルールのサブセットを表示するようにルールをフィルタ処理することによって、ルール状態やルール設定を変更するルールのセットを正確に選択できます。

ネットワーク上のホストとアプリケーションに関連付けられた脆弱性に基づいてルール状態推奨を生成し、オプションで、推奨状態を反映するようにルールを更新できます。

詳細については、次の項を参照してください。

- 「侵入防御ルール タイプについて」（P.21-2）では、侵入ポリシーで表示または設定可能な侵入ルールとプリプロセッサ ルールについて説明します。
- 「侵入ポリシー内のルールの表示」（P.21-3）では、[Rules] ページでルールの順序を変更したり、ページ上のアイコンを解釈したり、ルール詳細に焦点を当てたりするための方法について説明します。
- 「侵入ポリシー内のルールのフィルタ処理」（P.21-11）では、ルール フィルタを使用して、ルール設定を適用するルールを見つける方法について説明します。
- 「ルール状態の設定」（P.21-22）では、[Rules] ページでルールを有効または無効にする方法について説明します。
- 「ポリシー単位の侵入イベント通知のフィルタ処理」（P.21-25）では、特定のルールに対するイベント フィルタリングしきい値の設定方法と特定のルールの抑制方法について説明します。
- 「動的ルール状態の追加」（P.21-33）では、一致するトラフィックでレート異常が検出されたときに動的にトリガーとして使用されるルール状態の設定方法について説明します。
- 「アラートの追加」（P.21-36）では、SNMP アラートを特定のルールに関連付ける方法について説明します。
- 「詳細設定の自動有効化」（P.22-12）では、[Generate Events] または [Drop and Generate Events] に設定されたルールに必要なプリプロセッサとその他の高度な機能を有効にする方法について説明します。

- 「ルール コメントの追加」（P.21-38）では、侵入ポリシー内のルールにコメントを追加する方法について説明します。
- 「FireSIGHT ルール状態推奨の管理」（P.21-39）では、ネットワーク上のホストとアプリケーションに関連付けられた脆弱性に基づいてルール状態推奨を生成する方法について説明します。
- 「侵入ポリシーでのレイヤの使用」（P.23-1）では、ルール属性と詳細設定に関する個別の設定で構成された侵入ポリシー層を追加することによって、複雑なネットワークで複数の侵入ポリシーをより効率的に管理する方法について説明します。

侵入防御ルール タイプについて

ライセンス：Protection

侵入ポリシーには、侵入ルールとプリプロセッサ ルールという 2 つのルール タイプが含まれています。

侵入ルールは、ネットワーク上の脆弱性を悪用する試みを検出するキーワードと引数の指定されたセットで、ネットワーク トラフィックを分析してルール内の基準が満たされているかどうかをチェックします。システムが各ルール内で指定された条件とパケットを照らし合わせます。そして、パケット データとルール内で指定されたすべての条件が一致した場合に、ルールがトリガーとして使用されます。システムには、シスコ脆弱性調査チーム（VRT）が作成した次の 2 種類の侵入ルールが付属しています。共有オブジェクト ルールは、コンパイルされ、変更できません（送信元ポート、宛先ポート、IP アドレスなどのルール 見出し情報を除く）。標準テキスト ルールは、ルールの新しいカスタム インスタンスとして保存して変更できます。

システムには、プリプロセッサに関連付けられたルールであるプリプロセッサ ルールとパケット デコーダ検出オプションも付属しています。プリプロセッサ ルールはコピーまたは編集できません。ほとんどのプリプロセッサ ルールがデフォルトで無効になっているため、システムにプリプロセッサ ルールに対するイベントの生成とインライン展開での違反パケットの破棄を指示する場合は、これらのルールを有効にする（つまり、[Generate Events] または [Drop and Generate Events] に設定する）必要があります。

VRT が、システムに付属のデフォルト侵入ポリシー用のシスコの共有オブジェクト ルール、標準テキスト ルール、およびプリプロセッサ ルールのデフォルト ルール状態を決定します。

次の表に、FireSIGHT システムに付属しているルール タイプの説明を示します。

表 21-1　ルール タイプ

タイプ	説明
共有オブジェクト ルール	C ソース コードからコンパイルされたバイナリ モジュールとして配布されるシスコ脆弱性調査チーム（VRT）によって作成された侵入ルール。共有オブジェクト ルールを使用して、標準テキスト ルールでは不可能な方法で攻撃を検出できます。共有オブジェクト ルール内のルール キーワードと引数は変更できません。実行できるのは、ルール内で使用されている変数の変更か、送信元ポート、宛先ポート、IP アドレスなどの要素の変更とカスタム共有オブジェクト ルールとしてのルールの新しいインスタンスの保存のみです。共有オブジェクト ルールには、GID（ジェネレータ ID）の 3 が割り当てられます。詳細については、「既存のルールの変更」（P.32-110）を参照してください。
標準テキスト ルール	VRT によって作成された侵入ルール、コピーされて新しいカスタム ルールとして保存された侵入ルール、ルール エディタを使用して作成された侵入ルール、またはユーザがローカル マシン上で作成してインポートしたローカル ルールとしてインポートされた侵入ルール。VRT によって作成された標準ルール内のルール キーワードと引数は変更できません。実行できるのは、ルール内で使用されている変数の変更か、送信元ポート、宛先ポート、IP アドレスなどの要素の変更とカスタム標準テキスト ルールとしてのルールの新しいインスタンスの保存のみです。詳細については、「既存のルールの変更」（P.32-110）、「侵入ルールの概要と作成」（P.32-1）、および「ローカル ルール ファイルのインポート」（P.53-21）を参照してください。VRT によって作成された標準テキスト ルールには、GID（ジェネレータ ID）の 1 が割り当てられます。ルール エディタを使用して作成した、または、ローカル ルールとしてインポートしたカスタム標準テキスト ルールには 1000000 以上の SID（シグニチャ ID）が割り当てられます。
プリプロセッサ ルール	パケット デコーダの検出オプションまたは FireSIGHT システムに付属のプリプロセッサの 1 つに関連付けられたルール。プリプロセッサ ルールによってイベントを生成するには、プリプロセッサ ルールを有効にする必要があります。このルールには、デコーダ固有またはプリプロセッサ固有の GID（ジェネレータ ID）が割り当てられます。詳細については、「ジェネレータ ID」の表を参照してください。

侵入ポリシー内のルールの表示

ライセンス：Protection

侵入ポリシー内のルールの表示方法を調整できます。ルールはいくつかの基準に基づいてソートできます。特定のルールの詳細を表示して、ルール設定、ルール ドキュメント、およびその他のルール仕様を確認することもできます。

[Rules] ページには次の 4 つの主な機能領域があります。

- フィルタリング機能：詳細については、「侵入ポリシー内のルールのフィルタ処理」（P.21-11）を参照してください。
- ルール属性メニュー：詳細については、「ルール状態の設定」（P.21-22）、「ポリシー単位の侵入イベント通知のフィルタ処理」（P.21-25）、「動的ルール状態の追加」（P.21-33）、「アラートの追加」（P.21-36）、および「ルール コメントの追加」（P.21-38）を参照してください。
- ルール一覧：詳細については、「[Rules] ページのカラム」を参照してください。
- ルール詳細：詳細については、「ルール詳細の表示」（P.21-6）を参照してください。

さまざまな基準に基づいてルールをソートすることもできます。詳細については、「ルール画面のソート」（P.21-5）を参照してください。

カラム見出しとして使用されているアイコンは、設定項目にアクセスするためのメニュー バー内のメニューに対応していることに注意してください。たとえば、[Rule State] メニューは、[Rule State] カラムと同じアイコン（  ）でマークされています。

次の表に、[Rules] ページのカラムの説明を示します。

表 21-2　[Rules] ページのカラム

見出し	説明	詳細の参照先
GID	ルールのジェネレータ ID（GID）を表す整数。	「プリプロセッサのジェネレータ ID の読み取り」（P.22-9）
SID	ルールの一意の識別子として機能する Snort ID（SID）を表す整数。	「プリプロセッサのジェネレータ ID の読み取り」（P.22-9）
Message	このルールによって生成されるイベントに含まれるメッセージ。ルールの名前としても機能する。	「イベント メッセージの定義」（P.32-12）
	ルールのルール状態。次の 4 つの中のいずれか。 • ドロップしてイベントを生成する（） • イベントを生成する（  ） • 無効にする（） • 継承する（空白） ルール状態アイコンをクリックすることによって、ルールの [Set rule state] ダイアログボックスにアクセスできることに注意してください。	「ルール状態の設定」（P.21-22）
	ルールの FireSIGHT推奨ルール状態。	「FireSIGHT ルール状態推奨の管理」（P.21-39）
	ルールに適用されるイベントしきい値やイベント抑制などのイベント フィルタ。	「ポリシー単位の侵入イベント通知のフィルタ処理」（P.21-25）
	ルールの動的ルール状態。指定されたレート異常が発生した場合に有効になります。	「動的ルール状態の追加」（P.21-33）
	SNMP アラートを含む、ルールに対して設定されたアラート。	「アラートの追加」（P.21-36）
	ルールに追加されたコメント。	「ルール コメントの追加」（P.21-38）

階層ドロップダウン リストを使用して、ポリシー内の他の階層の [Rules] ページに切り替えることもできます。ポリシーに階層を追加しなかった場合にドロップダウン リストに表示される編集可能なビューはポリシーの [Rules] ページと、元は [My Changes] という名前だったポリシー層の [Rules] ページだけであることに注意してください。これらのビューの一方を変更すると、もう一方も同じように変更されることにも注意してください。詳細については、「侵入ポリシーでのレイヤの使用」（P.23-1）を参照してください。ドロップダウン リストには、読み取り専用の基本ポリシーの [Rules] ページも表示されます。基本ポリシーの詳細については、「基本ポリシーについて」（P.20-17）を参照してください。

侵入ポリシー内のルールを表示する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、「侵入ポリシー変更のコミット」（P.20-9）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Policy Information] ページで [Manage Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ナビゲーション パネルの境界線の上にある [Rules] を選択すると、同じルール一覧が表示されることに注意してください。このビューでポリシー内のすべてのルール属性を表示して設定できます。

ルール画面のソート

ライセンス：Protection

[Rules] ページでは、見出しタイトルまたはアイコンをクリックすることによって、ルールをいずれかのカラムでソートできます。

見出しまたはアイコン上の上矢印（▲）または下矢印（▼）は、そのカラムを基準として、その方向にソートが実行されることを意味していることに注意してください。

侵入ポリシー内でルールをソートする方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、「侵入ポリシー変更のコミット」（P.20-9）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Manage Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　ソートの基準とするカラムの一番上のタイトルまたはアイコンをクリックします。

ルールがそのカラムのカラム見出しに表示された矢印が示す方向でソートされます。反対方向でソートするには、見出しを再度クリックします。ソート順と矢印が反転します。

ルール詳細の表示

ライセンス：Protection

[Rule Detail] ビューで、ルール ドキュメント、FireSIGHT推奨、およびルール オーバーヘッドを表示できます。また、ルール固有の機能を表示および追加できます。

脆弱性にマップされていないローカル ルールにはオーバーヘッドがないことに注意してください。

表 21-3　ルールの詳細

項目	説明	詳細の参照先
Summary	ルールの概要。ルール ベースのイベントでは、ルール ドキュメントに概要情報が含まれている場合にこのローが表示されます。	「イベント情報の表示」（P.18-22）
Rule State	ルールの現在のルール状態。ルール状態が設定された階層も示します。	「ルール状態の設定」（P.21-22）、「侵入ポリシーでのレイヤの使用」（P.23-1）
FireSIGHT Recommendation	FireSIGHT推奨が生成されている場合のルールの推奨ルール状態。	「FireSIGHT ルール状態推奨の管理」（P.21-39）
Rule Overhead	システム パフォーマンスに対するルールの潜在的影響とルールが誤検出を引き起こす確率。	「ルール オーバーヘッドについて」（P.21-41）
Thresholds	このルールに現在設定されているしきい値と、ルールのしきい値を追加するための機能。	「ルールのしきい値の設定」（P.21-7）
Suppressions	このルールに現在設定されている抑制設定と、ルールの抑制を追加するための機能。	「ルールの抑制の設定」（P.21-8）
Dynamic State	このルールに現在設定されているレート ベースのルール状態と、ルールの動的ルール状態を追加するための機能。	「ルールの動的ルール状態の設定」（P.21-9）
Alerts	このルールに現在設定されているアラートと、ルールのアラートを追加するための機能。	「ルールの SNMP アラートの設定」（P.21-10）
Comments	このルールに追加されたコメントと、ルールのコメントを追加するための機能。	「ルールに関するルール コメントの追加」（P.21-10）
Documentation	シスコ脆弱性調査チーム（VRT）から提供される現在のルールのルール ドキュメント。	「パケット ビュー アクションの使用」（P.18-26）

ルール詳細を表示する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、「侵入ポリシー変更のコミット」（P.20-9）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Manage Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　ルール詳細を表示するルールを強調表示します。

ステップ 5　[Show details] をクリックします。

[Rule Detail] ビューが表示されます。詳細を再度非表示にするには、[Hide details] をクリックします。

ヒント　[Rules] ビューでルールをダブル クリックすることによって、[Rule Detail] を開くこともできます。

ルールのしきい値の設定

ライセンス：Protection

[Rule Detail] ページで、ルールの単一のしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。しきい値設定の詳細については、「イベントしきい値の設定」（P.21-25）を参照してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細でしきい値を設定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　しきい値の横にある [Add] をクリックします。

[Set Threshold] ダイアログボックスが表示されます。

ステップ 2　設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベント インスタンス数に通知を制限する場合は、[Limit] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[Threshold] を選択します。
- 指定されたイベント インスタンス数後に期間あたり 1 回ずつ通知を提供する場合は、[Both] を選択します。

ステップ 3　イベント インスタンスを送信元 IP アドレスと宛先 IP アドレスのどちらで追跡するかを指定するために [Track By] の該当するオプションを選択します。

ステップ 4　[Count] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

ステップ 5　[Seconds] フィールドに、イベント インスタンスを追跡する期間を指定する 1 ～ 86400 の数値を入力します。

ステップ 6　[OK] をクリックします。

システムが、しきい値を追加し、[Event Filtering] カラムのルールの横にイベント フィルタ アイコン（）を表示します。ルールに複数のイベント フィルタを追加すると、アイコン上にイベント フィルタの数が表示されます。

ルールの抑制の設定

ライセンス：Protection

[Rule Detail] ページで、ルールの 1 つまたは複数の抑制を設定できます。抑制の詳細については、「侵入ポリシー単位の抑制の設定」（P.21-30）を参照してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細で抑制を設定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　抑制の横にある [Add] をクリックします。

[Add Suppression] ダイアログボックスが表示されます。

ステップ 2　次の [Suppression Type] オプションのいずれかを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[Rule] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[Source] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[Destination] を選択します。

ステップ 3　抑制タイプとして [Source] または [Destination] を選択した場合は、[Network] フィールドに IP アドレス、アドレス ブロック、またはそれらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。侵入ポリシーがアクセス コントロール ポリシーのデフォルト アクションに関連付けられている場合は、デフォルト アクション変数セットでネットワーク変数を指定または列挙することもできます。

FireSIGHT システムで IPv4 CIDR と IPv6 プレフィクス長アドレス ブロックを使用する方法については、「IP アドレスの表記法」（P.1-19）を参照してください。

ステップ 4　[OK] をクリックします。

システムが、抑制条件を追加し、抑制するルールの横にある [Event Filtering] カラムのルールの横にイベント フィルタ アイコン（）を表示します。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

ルールの動的ルール状態の設定

ライセンス：Protection

[Rule Detail] ページで、ルールの 1 つまたは複数の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2 つの動的ルール状態が競合している場合は、最初のアクションが実行されることに注意してください。動的ルール状態の詳細については、「動的ルール状態について」（P.21-33）を参照してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細で動的ルール状態を設定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　動的状態の横にある [Add] をクリックします。

[Add Rate-Based Rule State] ダイアログボックスが表示されます。

ステップ 2　ルール一致の追跡方法を指定するために、該当する [Track By] オプションを選択します。

- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[Source] を選択します。
- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[Destination] を選択します。
- そのルールのすべての一致を追跡する場合は、[Rule] を選択します。

ステップ 3　オプションで、[Track By] を [Source] または [Destination] に設定した場合は、[Network] フィールドに追跡する各ホストの IP アドレスを入力します。

FireSIGHT システムで IPv4 CIDR と IPv6 プレフィクス長表記を使用する方法については、「IP アドレスの表記法」（P.1-19）を参照してください。

ステップ 4　攻撃レートを設定する期間あたりのルール一致数を指定します。

- [Count] フィールドで、1 ～ 2147483647 の整数を使用して、しきい値として使用するルール一致の数を指定します。
- [Seconds] フィールドで、1 ～ 2147483647 の整数を使用して、攻撃を追跡する期間を表す秒数を指定します。

ステップ 5　条件が満たされたときに実行すべき新しいアクションを指定する場合は、[New State] オプション ボタンを選択します。

- イベントを生成する場合は、[Generate Events] を選択します。
- インライン展開でイベントを生成し、イベントをトリガーしたパケットを破棄する場合、または、パッシブ展開でイベントを生成する場合は、[Drop and Generate Events] を選択します。
- アクションを実行しない場合は、[Disabled] を選択します。

ステップ 6　[Timeout] フィールドに、1 ～ 2147483647（約 68 年）の整数を使用して、新しいアクションを有効にしておく秒数を入力します。タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションがタイムアウトしないようにする場合は、0 を指定します。

ステップ 7　[OK] をクリックします。

システムが、動的ルール状態を追加し、[Dynamic State] カラムのルールの横に動的状態アイコン（  ）を表示します。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

必須フィールドを空白にした場合は、フィールドに値を入力する必要があることを伝えるエラー メッセージが表示されます。

ルールの SNMP アラートの設定

ライセンス：Protection

[Rule Detail] ページで、ルールの SNMP アラートを設定できます。SNMP アラートの詳細については、「アラートの追加」（P.21-36）を参照してください。

ルール詳細で SNMP アラートを追加する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　アラートの横にある [Add SNMP Alert] をクリックします。

システムが、アラートを追加し、[Alerting] カラムのルールの横にアラート アイコン（  ）を表示します。ルールに複数のアラートを追加した場合は、アイコン上にアラートの数が表示されます。

ルールに関するルール コメントの追加

ライセンス：Protection

[Rule Detail] ページで、ルールに関するルール コメントを追加できます。ルール コメントの詳細については、「ルール コメントの追加」（P.21-38）を参照してください。

ルール詳細でコメントを追加する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　コメントの横にある [Add] をクリックします。

[Add Comment] ダイアログボックスが表示されます。

ステップ 2　ルール コメントを入力します。

ステップ 3　[OK] をクリックします。

システムが、コメントを追加し、[Comments] カラムのルールの横にコメント アイコン（  ）を表示します。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

ヒント　ルール コメントを削除するには、ルール コメント セクションで [Delete] をクリックします。侵入ポリシーの変更がコミットされていないコメントがキャッシュされている場合にだけ、コメントを削除できることに注意してください。侵入ポリシーの変更がコミットされた後は、ルール コメントを削除できなくなります。

侵入ポリシー内のルールのフィルタ処理

ライセンス：Protection

[Rules] ページに表示するルールは、1 つの基準または 1 つ以上の基準の組み合わせに基づいてフィルタ処理できます。

作成したフィルタが [Filter] テキスト ボックスに表示されます。フィルタ パネルでキーワードとキーワード引数をクリックしてフィルタを作成できます。複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[Category] で [preprocessor] を選択してから、[Rule Content] > [GID] の順に選択して、「116」と入力すると、プリプロセッサ ルールで、**かつ**、GID が 116 のすべてのルールを取得する「`Category: "preprocessor" GID:"116"`」というフィルタが返されます。

Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific、Preprocessor、および Priority の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、Shift キーを押しながら、[Category] から [os-linux] と [os-windows] を選択すれば、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,os-linux"`」というフィルタを作成できます。

フィルタ パネルを表示するには、表示アイコン（  ）をクリックします。

フィルタ パネルを非表示にするには、非表示アイコン（  ）をクリックします。

詳細については、次のトピックを参照してください。

- 「侵入ポリシー内のルール フィルタ処理について」（P.21-11）
- 「侵入ポリシー内のルール フィルタの設定」（P.21-21）

侵入ポリシー内のルール フィルタ処理について

ライセンス：Protection

ルール フィルタ キーワードは、ルール状態やイベント フィルタなどのルール設定を適用するルールを見つけやすくします。[Rules] ページのフィルタ パネルで必要な引数を選択することによって、キーワードでフィルタ処理すると同時に、キーワードの引数を選択することができます。

詳細については、次の項を参照してください。

- 「侵入ポリシー ルール フィルタを作成するためのガイドライン」（P.21-12）
- 「ルール構成フィルタについて」（P.21-15）
- 「ルール コンテンツ フィルタについて」（P.21-17）
- 「ルール カテゴリについて」（P.21-19）
- 「ルール フィルタのを直接編集」（P.21-20）

侵入ポリシー ルール フィルタを作成するためのガイドライン

ライセンス：Protection

ほとんどの場合、フィルタを作成するときに、侵入ポリシー内の [Rules] ページの左側にあるフィルタ パネルを使用して必要なキーワード/引数を選択できます。

フィルタ パネルでは、ルール フィルタがルール フィルタ グループに分類されます。多くのルール フィルタ グループにサブ基準が含まれているため、探している特定のルールを簡単に見つけることができます。一部のルール フィルタには、展開して個別のルールにドリルダウンするための複数のレベルが設定されています。

フィルタ パネル内の項目は、場合によって、フィルタ タイプ グループを表したり、キーワードを表したり、キーワードの引数を表したりします。次の経験則をフィルタの作成に役立ててください。

- キーワード（Rule Configuration、Rule Content、Platform Specific、および Priority）以外のフィルタ タイプ グループ見出しを選択すると、そのグループが展開して使用可能なキーワードが一覧表示されます。

  基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ処理する引数を指定するためのポップアップ ウィンドウが表示されます。

  そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

  たとえば、フィルタ パネルの [Rule Configuration] > [Recommendation] で [Drop and Generate Events] をクリックすると、「`Recommendation:"Drop and Generate Events"`」がフィルタ テキスト ボックスに追加されます。その後で、[Rule Configuration] > [Recommendation] で [Generate Events] をクリックすると、フィルタが「`Recommendation:"Generate Events"`」に変更されます。

- キーワード（Category、Classifications、Microsoft Vulnerabilities、Microsoft Worms、Priority、および Rule Update）になっているフィルタ タイプ グループ見出しを選択すると、使用可能な引数が一覧表示されます。

  このタイプのグループから項目を選択すると、適用される引数とキーワードがすぐにフィルタに追加されます。キーワードがすでにフィルタ内に存在していた場合は、そのグループに対応するキーワードの既存の引数が置き換えられます。

  たとえば、フィルタ パネルの [Category] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキスト ボックスに追加されます。その後で、[Category] で [os-windows] をクリックすると、フィルタが「`Category:"os-windows"`」に変更されます。

- [Rule Content] の下の [Reference] はキーワードであり、その下に特定の参照 ID タイプが列挙されます。参照キーワードのいずれかを選択すると、引数を指定するためのポップアップ ウィンドウが表示され、キーワードが既存のフィルタに追加されます。キーワードがすでにフィルタ内で使用されていた場合は、既存の引数が指定した新しい引数に置き換えられます。

  たとえば、フィルタ パネルで [Rule Content] > [Reference] > [CVE ID] の順にクリックすると、ポップアップ ウィンドウが開いて CVE ID を指定するよう示されます。「`2007`」と入力すると、「`CVE:"2007"`」がフィルタ テキスト ボックスに追加されます。別の例では、フィルタ パネルで [Rule Content] > [Reference] の順にクリックすると、ポップアップ ウィンドウが開いて、参照を指定するよう示されます。「`2007`」と入力すると、「`Reference:"2007"`」がフィルタ テキスト ボックスに追加されます。

- 複数のグループからルール フィルタ キーワードを選択した場合は、各フィルタ キーワードがフィルタに追加され、既存のキーワードが維持されます（同じキーワードの新しい値で上書きされなかった場合）。

  たとえば、フィルタ パネルの [Category] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキスト ボックスに追加されます。その後で、[Microsoft Vulnerabilities] で [MS00-006] をクリックすると、フィルタが「`Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`」に変更されます。

- 複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[Category] で [preprocessor] を選択してから、[Rule Content] > [GID] の順に選択して、「`116`」と入力すると、プリプロセッサ ルールで、**かつ**、GID が 116 のすべてのルールを取得する「`Category: "preprocessor" GID:"116"`」というフィルタが返されます。

- Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific、および Priority の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、Shift キーを押しながら、[Category] から [os-linux] と [os-windows] を選択すれば、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,app-detect"`」というフィルタを作成できます。

複数のフィルタ キーワード/引数のペアで同じルールが取得される場合があります。たとえば、ルールが **dos** カテゴリでフィルタ処理された場合と High 優先度でフィルタ処理された場合はともに、DOS Cisco attempt rule（SID 1545）が表示されます。

注　シスコ VRT がルール更新メカニズムを使用してルール フィルタを追加または削除する場合があります。

[Rules] ページ上のルールは、共有オブジェクト ルール（ジェネレータ ID 3）と標準テキスト ルール（ジェネレータ ID 1）のどちらかであることに注意してください。次の表に、さまざまなルール フィルタの説明を示します。

表 21-4　ルール フィルタ グループ

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
Rule Configuration	ルールの設定に基づいてルールを検索します。「ルール構成フィルタについて」（P.21-15）を参照してください。	いいえ	グループ	キーワード
Rule Content	ルールの内容に基づいてルールを検索します。「ルール コンテンツ フィルタについて」（P.21-17）を参照してください。	いいえ	グループ	キーワード
Category	ルール エディタで使用されるルール カテゴリに基づいてルールを検索します。ローカル ルールはローカル サブグループに表示されることに注意してください。「ルール カテゴリについて」（P.21-19）を参照してください。	はい	キーワード	引数

表 21-4　ルール フィルタ グループ（続き）

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
Classifications	ルールによって生成されるイベントのパケット画面内に表示される攻撃分類に基づいてルールを検索します。「侵入イベントの検索」（P.18-39）および「侵入イベント分類の定義」（P.32-13）を参照してください。	いいえ	キーワード	引数
Microsoft Vulnerabilities	Microsoft セキュリティ情報番号に従ってルールを検索します。	はい	キーワード	引数
Microsoft Worms	Microsoft Windows ホストに影響する特定のワームに基づいてルールを検索します。	はい	キーワード	引数
Platform Specific	オペレーティング システムの特定のバージョンとの関連性に基づいてルールを検索します。 ルールが複数のオペレーティング システムまたは 1 つのオペレーティング システムの複数のバージョンに影響する場合があることに注意してください。たとえば、SID 2260 を有効にすると、Mac OS X、IBM AIX、およびその他のオペレーティング システムの複数のバージョンに影響します。	はい	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
Preprocessors	個別のプリプロセッサのルールを検索します。 プリプロセッサが有効になっている場合にプリプロセッサ オプションに対するイベントを生成するためには、そのオプションに関連付けられたプリプロセッサ ルールを有効にする必要があることに注意してください。詳細については、「プリプロセッサについて」（P.22-5）および「ルール状態の設定」（P.21-22）を参照してください。	はい	グループ	サブグループ
Priority	高、中、および低の優先度に基づいてルールを検索します。 ルールに割り当てられた分類によってその優先度が決定されます。これらのグループは、さらにルール カテゴリに分類されます。ローカル ルール（つまり、ユーザが作成したルール）は優先度グループに表示されないことに注意してください。	はい	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
Rule Update	特定のルール更新を通して追加または変更されたルールを検索します。ルール更新ごとに、更新内のすべてのルール、更新でインポートされた唯一の新しいルール、または更新によって変更された唯一の既存のルールを表示します。	いいえ	キーワード	引数

ルール構成フィルタについて

ライセンス：Protection

[Rules] ページに表示されたルールをいくつかのルール構成設定でフィルタ処理できます。たとえば、ルール状態が推奨ルール状態と一致しない一連のルールを表示する場合は、[Does not match recommendation] を選択することによってルール状態をフィルタ処理できます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ処理する引数を指定するためのポップアップ ウィンドウが表示されます。

そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [Rule Configuration] > [Recommendation] で [Drop and Generate Events] をクリックすると、「`Recommendation:"Drop and Generate Events"`」がフィルタ テキスト ボックスに追加されます。その後で、[Rule Configuration] > [Recommendation] で [Generate Events] をクリックすると、フィルタが「`Recommendation:"Generate Events"`」に変更されます。

フィルタ処理に使用可能なルール構成設定に関する詳細については、次の手順を参照してください。

ルール状態フィルタを使用する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Rule Configuration] で、[Rule State] をクリックします。

ステップ 2　フィルタ処理するルール状態を選択します。

- イベントを生成するだけのルールを検索するには、[Generate Events] を選択して、[OK] をクリックしてします。
- イベントを生成して一致するパケットをドロップするルールを検索するには、[Drop and Generate Events] を選択して、[OK] をクリックします。
- 無効になっているルールを検索するには、[Disabled] を選択して、[OK] をクリックします。
- ルール状態が推奨状態と一致しないルールを検索するには、[Does not match recommendation] を選択して、[OK] をクリックします。

最新のルール状態に基づいてルールを表示するように [Rules] ページが更新されます。

推奨フィルタを使用する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Rule Configuration] で、[Recommendation] をクリックします。

ステップ 2　フィルタ処理する FireSIGHT ルール状態推奨を選択します。

推奨ルール状態に基づいてルールを表示するように [Rules] ページが更新されます。

しきい値フィルタを使用する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Rule Configuration] で、[Threshold] をクリックします。

ステップ 2　フィルタ処理するしきい値設定を選択します。

- しきい値タイプが `limit` のルールを検索するには、[Limit] を選択して、[OK] をクリックします。
- しきい値タイプが `threshold` のルールを検索するには、[Threshold] を選択して、[OK] をクリックします。
- しきい値タイプが `both` のルールを検索するには、[Both] を選択して、[OK] をクリックします。
- しきい値が送信元によって追跡されるルールを検索するには、[Source] を選択して、[OK] をクリックします。
- しきい値が宛先によって追跡されるルールを検索するには、[Destination] を選択して、[OK] をクリックします。
- しきい値が設定されたすべてのルールを検索するには、[All] を選択して、[OK] をクリックします。

フィルタで指定されたしきい値のタイプがルールに適用されているルールを表示するように [Rules] ページが更新されます。

抑制フィルタを使用する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Rule Configuration] で、[Suppression] をクリックします。

ステップ 2　フィルタ処理する抑制設定を選択します。

- イベントがそのルールによって検査されるパケットに抑制されたルールを検索するには、[Rule] を選択して、[OK] をクリックします。
- イベントがトラフィックの送信元に基づいて抑制されるルールを検索するには、[Source] を選択して、[OK] をクリックします。
- イベントがトラフィックの宛先に基づいて抑制されるルールを検索するには、[Destination] を選択して、[OK] をクリックします。
- 抑制が設定されたすべてのルールを検索するには、[All] を選択して、[OK] をクリックします。

フィルタで指定された抑制のタイプがルールに適用されているルールを表示するように [Rules] ページが更新されます。

動的状態フィルタを使用する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Rule Configuration] で、[Dynamic State] をクリックします。

ステップ 2　フィルタ処理する抑制設定を選択します。

- 動的状態がそのルールによって検査されるパケットに設定されたルールを検索するには、[Rule] を選択して、[OK] をクリックします。
- 動的状態がトラフィックの送信元に基づくパケットに設定されたルールを検索するには、[Source] を選択して、[OK] をクリックします。
- 動的状態がトラフィックの宛先に基づいて設定されたルールを検索するには、[Destination] を選択して、[OK] をクリックします。
- [Generate Events] の動的状態が設定されたルールを検索するには、[Generate Events] を選択して、[OK] をクリックします。
- [Drop and Generate Events] の動的状態が設定されたルールを検索するには、[Drop and Generate Events] を選択して、[OK] をクリックします。
- [Disabled] の動的状態が設定されたルールを検索するには、[Disabled] を選択して、[OK] をクリックします。
- 抑制が設定されたすべてのルールを検索するには、[All] を選択して、[OK] をクリックします。

フィルタで指定された動的ルール状態がルールに適用されているルールを表示するように [Rules] ページが更新されます。

コメント フィルタを使用する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Rule Configuration] で、[Comment] をクリックします。

ステップ 2　フィルタ処理するコメント テキストの文字列を入力します。

ルールに適用されるコメントにフィルタで指定された文字列が含まれているルールを表示するように [Rules] ページが更新されます。

ルール コンテンツ フィルタについて

ライセンス：Protection

[Rules] ページに表示されたルールをいくつかのルール コンテンツ項目でフィルタ処理できます。たとえば、ルール SID を検索することによって、ルールをすばやく取得できます。特定の宛先ポートに送信されるトラフィックを検査するすべてのルールを検索することもできます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ処理する引数を指定するためのポップアップ ウィンドウが表示されます。

そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [Rule Content] で [SID] をクリックすると、ポップアップ ウィンドウが開いて SID の入力が促されます。「1045」と入力すると、「SID:"1045"」がフィルタ テキスト ボックスに追加されます。その後で、再度 [SID] をクリックして、SID フィルタを「1044」に変更すると、フィルタが「SID:"1044"」に変更されます。

フィルタ処理に使用可能なルール コンテンツの詳細については、次の表を参照してください。

表 21-5　ルール コンテンツ フィルタ

このフィルタを使用する場合のクリック対象	次の操作	結果
Message	フィルタ処理するメッセージ文字列を入力して、[OK] をクリックします。	メッセージ フィールドで指定された文字列を含むルールを検索します。
SID	フィルタ処理する SID 番号を入力して、[OK] をクリックします。	指定された SID が割り当てられたルールを検索します。
GID	フィルタ処理する GID 番号を入力して、[OK] をクリックします。	指定された GID が割り当てられたルールを検索します。
Reference	フィルタ処理する参照文字列を入力して、[OK] をクリックします。	参照フィールドで指定された文字列を含むルールを検索します。
Action	フィルタ処理するアクションを選択します。 • アラート ルールを検索するには、[Alert] を選択して、[OK] をクリックします。 • パス ルールを検索するには、[Pass] を選択して、[OK] をクリックします。	alert または pass で始まるルールを検索します。
Protocol	フィルタ処理するプロトコルを選択します。	選択されたプロトコルを含むルールを検索します。
Direction	フィルタ処理する方向設定を選択します。 • 特定の方向に移動するトラフィックを検査するルールを検索するには、[Directional] を選択して、[OK] をクリックします。 • 送信元と宛先の間をどちらの方向にも移動するトラフィックを検査するルールを検索するには、[Bidirectional] を選択して、[OK] をクリックしてします。	ルールに、指定された方向設定が含まれているかどうかに基づいてルールを検索します。
Source IP	フィルタ処理する送信元 IP アドレスを入力します。 有効な IP アドレス、CIDR ブロック/プレフィクス長、または $HOME_NET や $EXTERNAL_NET などの変数を使用してフィルタ処理できることに注意してください。	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用するルールを検索します。

表 21-5　ルール コンテンツ フィルタ （続き）

このフィルタを使用する場合のクリック対象	次の操作	結果
Destination IP	フィルタ処理する宛先 IP アドレスを入力します。 有効な IP アドレス、CIDR ブロック/プレフィクス長、または $HOME_NET や $EXTERNAL_NET などの変数を使用してフィルタ処理できることに注意してください。	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用するルールを検索します。
Source port	フィルタ処理する送信元ポートを入力します。ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。	指定された送信元ポートを含むルールを検索します。
Destination port	フィルタ処理する宛先ポートを入力します。ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。	指定された宛先ポートを含むルールを検索します。
Rule Overhead	フィルタ処理するルール オーバーヘッドの量を選択します。	選択されたルール オーバーヘッドを伴うルールを検索します。
Metadata	フィルタ処理するメタデータ キーと値のペアをスペースで区切って入力します。 たとえば、HTTP アプリケーション プロトコルに関連するメタデータを使用したルールを検索するには、「metadata:"service http"」と入力します。	一致するキーと値のペアを含むメタデータを使用したルールを検索します。

ルール カテゴリについて

ライセンス：Protection

FireSIGHT システムは、ルールが検出するトラフィックのタイプに基づいてカテゴリにルールを配置します。[Rules] ページで、ルール カテゴリでフィルタ処理することによって、カテゴリ内のすべてのルールにルール属性を設定できます。たとえば、ネットワーク上に Linux ホストが存在しない場合は、**os-linux** カテゴリでフィルタ処理してから、表示されたすべてのルールを無効にすることによって、**os-linux** カテゴリ全体を無効にすることができます。

カテゴリ名の上にポインタを移動すると、そのカテゴリ内のルールの数を表示できます。

注　シスコ VRT がルール更新メカニズムを使用してルール カテゴリを追加または削除する場合があります。

ルール フィルタのを直接編集

ライセンス：Protection

フィルタ パネルでフィルタをクリックしたときに入力される特殊なキーワードとその引数を変更するようにフィルタを編集できます。[Rules] ページのカスタム フィルタはルール エディタで使用されるものと同様に機能しますが、フィルタ パネルを通してフィルタを選択したときに表示される構文を使用して、[Rules] ページのフィルタに入力されたキーワードのいずれかを使用することもできます。今後使用するキーワードを決定するには、右側のフィルタ パネルで該当する引数をクリックします。フィルタ キーワードと引数構文がフィルタ テキスト ボックスに表示されます。

特定の値のみをサポートするキーワードの引数のリストを表示するには、「ルール構成フィルタについて」（P.21-15）、「ルール コンテンツ フィルタについて」（P.21-17）、および「ルール カテゴリについて」（P.21-19）を参照してください。キーワードのカンマ区切りの複数の引数は Category と Priority のフィルタ タイプでしかサポートされないことに注意してください。

引用符内のキーワードと引数、文字列、およびリテラル文字列と一緒に、複数のフィルタ条件を区切るスペースを使用できます。ただし、正規表現、ワイルドカード文字、または否定文字（!）、大なり記号（>）、小なり記号（<）などの特殊な演算子を含めることはできません。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[Category]、[Message]、および [SID] の各フィールドで指定された単語が検索されます。

キーワード、キーワード引数、および文字列では、いずれも大文字と小文字が区別されません。`gid` キーワードと `sid` キーワードを除くすべての引数と文字列が部分文字列として扱われます。`gid` と `sid` の引数は完全一致のみを返します。

ルール フィルタごとに、次の形式で 1 つ以上のキーワードを含めることができます。

`Keyword:"argument"`

ここで、*`Keyword`* は「ルール タイプ」の表に示すフィルタ グループ内のキーワードのいずれかで、*`argument`* は二重引用符で囲まれ、キーワードに関連した特定のフィールド内で検索される単一の大文字と小文字が区別されない英数字文字列です。キーワードは先頭文字を大文字にして入力する必要があることに注意してください。

`gid` と `sid` を除くすべてのキーワードの引数が部分文字列として扱われます。たとえば、引数の `123` は、`"12345"`、`"41235"`、`"45123"` などを返します。`gid` と `sid` の引数は完全一致のみを返します。たとえば、`sid:3080` は `SID 3080` のみを返します。

各ルール フィルタに、1 つ以上の英数字文字列を含めることもできます。文字列はルールの [Message] フィールド、シグニチャ ID、およびジェネレータ ID を検索します。たとえば、文字列 `123` は、ルール メッセージ内の文字列 `"Lotus123"` や `"123mania"` などを返し、`SID 6123` や `SID 12375` なども返します。ルールの [Message] フィールドの詳細については、「イベント メッセージの定義」（P.32-12）を参照してください。ルールの SID と GID の詳細については、「プリプロセッサのジェネレータ ID の読み取り」（P.22-9）を参照してください。1 つ以上の文字列でフィルタ処理することによって、SID を部分的に検索できます。

すべての文字列で大文字と小文字が区別されず、部分文字列として扱われます。たとえば、文字列 `ADMIN`、`admin`、または `Admin` はいずれも `"admin"`、`"CFADMIN"`、`"Administrator"` などを返します。

完全一致を返す場合は、文字列を引用符で囲む必要があります。たとえば、引用符付きのリテラル文字列 `"overflow attempt"` は完全一致のみを返しますが、引用符なしの 2 つの文字列 `overflow` と `attempt` で構成されたフィルタは `"overflow attempt"`、`"overflow multipacket attempt"`、`"overflow with evasion attempt"` などを返します。

キーワード、文字列、またはその両方の組み合わせをスペースで区切って入力することによって、フィルタ結果を絞り込むことができます。結果には、すべてのフィルタ条件と一致するすべてのルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のすべてのフィルタが同じルールを返します。

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

侵入ポリシー内のルール フィルタの設定

ライセンス：Protection

[Rules] ページで、ルールのサブセットを表示するようにルールをフィルタ処理できます。その後で、いずれかのページ機能を使用できます。これには、コンテキスト メニューで使用可能な機能の選択も含まれます。これは、特定のカテゴリのすべてのルールのしきい値を設定する場合などに便利です。フィルタ処理されたリスト内のルールとフィルタ処理されていないリスト内のルールで同じ機能を使用できます。たとえば、新しいルール状態を、フィルタ処理されたリスト内のルールまたはフィルタ処理されていないリスト内のルールに適用できます。

侵入ポリシー内の [Rules] ページの左側にあるフィルタ パネルから事前定義のフィルタ キーワードを選択できます。フィルタを選択すると、ページに、すべての一致するルールが表示されるか、どのルールも一致しなかったことが表示されます。

使用可能なすべてのキーワードと引数の詳細と、フィルタ パネルでのフィルタの作成方法については、「侵入ポリシー内のルール フィルタ処理について」（P.21-11）を参照してください。

フィルタにキーワードを追加してさらに絞り込むことができます。入力されたすべてのフィルタが、ルール データベース全体を検索して、一致するすべてのルールを返します。ページに前回のフィルタ結果が表示されている状態でフィルタを入力すると、ページが消去され、代わりに新しいフィルタの結果が返されます。

また、フィルタを選択したとき、または、フィルタを選択後にその中の引数値を変更したときに指定したものと同じキーワードと引数の構文を使用してフィルタを入力することもできます。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[Category]、[Message]、および [SID] の各フィールドで指定された単語が検索されます。

侵入ポリシー内の特定のルールに対してフィルタ処理する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、「侵入ポリシー変更のコミット」（P.20-9）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Manage Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。フィルタ内に存在するキーワードの引数をクリックすると、既存の引数が置き換えられることに注意してください。詳細については、次の各項を参照してください。

- 「侵入ポリシー ルール フィルタを作成するためのガイドライン」（P.21-12）
- 「ルール構成フィルタについて」（P.21-15）
- 「ルール コンテンツ フィルタについて」（P.21-17）
- 「ルール カテゴリについて」（P.21-19）
- 「ルール フィルタのを直接編集」（P.21-20）

ページが、すべての一致するルールを表示するように更新され、フィルタと一致するルールの数がフィルタ テキスト ボックスの上に表示されます。

ステップ 5　新しい設定を適用する 1 つ以上のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　オプションで、通常ページで行うような変更をルールに対して行えます。詳細については、次の項を参照してください。

- [Rules] ページ上でルールを有効または無効にする方法については、「ルール状態の設定」（P.21-22）を参照してください。
- ルールにしきい値設定と抑制を追加する方法については、「ポリシー単位の侵入イベント通知のフィルタ処理」（P.21-25）を参照してください。
- 一致するトラフィックでレート異常が発生したときにトリガされる動的ルール状態を設定する方法については、「動的ルール状態の追加」（P.21-33）を参照してください。
- 特定のルールに SNMP アラートを追加する方法については、「アラートの追加」（P.21-36）を参照してください。
- ルールにルール コメントを追加する方法については、「ルール コメントの追加」（P.21-38）を参照してください。

ステップ 7　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、「一般的な侵入ポリシー編集操作」の表を参照してください。

ルール状態の設定

ライセンス：Protection

シスコ脆弱性調査チーム（VRT）が、各デフォルト ポリシー内の侵入ルールとプリプロセッサ ルールのデフォルト状態を設定します。たとえば、ルールを Security over Connectivity デフォルト ポリシーでは有効にして、Connectivity over Security デフォルト ポリシーでは無効にすることができます。作成された侵入ポリシー ルールは、作成時に使用されたデフォルト ポリシー内のルールのデフォルト状態を継承します。

ルールを [Generate Events]、[Drop and Generate Events]、または [Disable] に個別に設定することも、状態を変更するルールを選択するためのさまざまな要素でルールをフィルタ処理することもできます。インライン展開では、インライン侵入展開で [Drop and Generate Events] ルール状態を使用して悪意のあるパケットをドロップできます。[Drop and Generate Events] ルール状態のルールはイベントを生成しますが、3D9900 または シリーズ 3 デバイスのインライン インターフェイス セットがタップ モードの場合を含むパッシブ展開ではパケットをドロップしないことに注意してください。ルールを [Generate Events] または [Drop and Generate Events] に設定すると、ルールが有効になります。ルールを [Disable] に設定すると、ルールが無効になります。

2 つのシナリオについて考えてみます。最初のシナリオでは、特定のルールのルール状態が [Generate Events] に設定されます。悪意のあるパケットがネットワークを通過してルールをトリガーすると、そのパケットが宛先に送信され、システムが侵入イベントを生成します。2 つ目のシナリオでは、同じルールのルール状態が、インライン展開で [Drop and Generate Events] に設定されていると仮定します。この場合は、悪意のあるパケットがネットワークを通過すると、システムがそのパケットをドロップして、侵入イベントを生成します。パケットがターゲットに到達することはありません。

侵入ポリシーでは、ルールの状態を次のいずれかに設定できます。

- システムで特定の侵入試行を検出して、一致したトラフィックが見つかった時点で侵入イベントを生成する場合は、ルール状態を [Generate Events] に設定します。
- システムで特定の侵入試行を検出してから、インライン展開で一致するトラフィックが見つかった時点で攻撃を含むパケットをドロップし、侵入イベントを生成する場合、あるいは、3D9900 または シリーズ 3 デバイスのインライン インターフェイス セットがタップ モードの場合を含むパッシブ展開で一致するトラフィックが見つかった時点で侵入イベントを生成する場合は、ルール状態を [Drop and Generate Events] に設定します。

  システムでパケットをドロップする場合は、インライン展開で侵入ポリシーを廃棄ルールに設定する必要があることに注意してください。詳細については、「インライン展開での破棄動作の設定」（P.20-15）を参照してください。
- システムで一致するトラフィックを評価しない場合は、ルール状態を [Disable] に設定します。

廃棄ルールを使用するには、次の手順を実行する必要があります。

- 侵入ポリシーで [Drop when Inline] オプションを有効にします。
- ルールと一致するすべてのパケットをドロップする必要があるすべてのルールのルール状態を [Drop and Generate Events] に設定します。
- 侵入ポリシーに関連付けられたアクセス コントロール ルールを含むアクセス コントロール ポリシーを、インライン セットを使用する管理対象デバイスに適用します。

[Rules] ページのルールのフィルタ処理は、廃棄ルールとして設定するルールを探すときに役立ちます。詳細については、「侵入ポリシー内のルールのフィルタ処理」（P.21-11）を参照してください。

ルール構造、ルール キーワードとそのオプション、およびルール作成構文については、「侵入ルールの概要と作成」（P.32-1）を参照してください。

VRT がルール更新を使用してデフォルト ポリシー内の 1 つ以上のルールのデフォルト状態を変更する場合があります。ルール更新での基本ポリシーの更新を許可すると、ポリシーの作成時に使用されたデフォルト ポリシー（または基礎となるデフォルト ポリシー）のデフォルト状態が変更されたときの、そのポリシー内のルールのデフォルト状態の変更も許可することになります。ただし、ルール状態を変更している場合は、ルール更新でその変更が上書きされないことに注意してください。

1 つ以上のルールのルール状態を変更する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、「侵入ポリシー変更のコミット」（P.20-9）を参照してください。

[Policy Information] ページが表示されます。

このページには、有効なルールの総数、[Generate Events] に設定された有効なルールの総数、および [Drop and Generate Events] に設定された有効なルールの総数が表示されることに注意してください。また、パッシブ展開では、[Drop and Generate Events] に設定されたルールで行われるのはイベントの生成のみであることにも注意してください。

ステップ 3　[Policy Information] ページで [Manage Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　ルール状態を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、「侵入ポリシー内のルール フィルタ処理について」（P.21-11）および「侵入ポリシー内のルール フィルタの設定」（P.21-21）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　ルール状態を設定する 1 つ以上のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　次の選択肢があります。

- トラフィックが選択されたルールと一致したときにイベントを生成するには、[Rule State] > [Generate Events] の順に選択します。
- インライン展開でトラフィックが選択されたルールと一致したときにイベントを生成し、そのトラフィックをドロップするには、[Rule State] > [Drop and Generate Events] の順に選択します。
- 選択されたルールと一致するトラフィックを検査しないようにするには、[Rule State] > [Disable] の順に選択します。

注　シスコでは、侵入ポリシー内のすべての侵入ルールを有効に**しない**ことを**強く**推奨しています。すべてのルールが有効になっている場合は、管理対象デバイスのパフォーマンスが低下する可能性があります。代わりに、できるだけネットワーク環境に合わせてルール セットを調整してください。

ステップ 7　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、「一般的な侵入ポリシー編集操作」の表を参照してください。

ポリシー単位の侵入イベント通知のフィルタ処理

ライセンス：Protection

侵入イベントの重要度は、発生頻度、送信元 IP アドレス、または宛先 IP アドレスに基づいて設定できます。イベントが特定の回数発生するまで注意が必要ない場合もあります。たとえば、何者かがサーバにログインしようとしても、特定の回数失敗するまで、気にする必要はありません。一方、ほんの少数の発生を見れば、広範な問題があることを理解できる場合もあります。たとえば、Web サーバに対して DoS 攻撃が行われた場合は、少数の侵入イベントの発生を確認しただけで、その状況に対処しなければならないことが分かります。同じイベントが何百回も確認されれば、システムの機能が麻痺します。

詳細については、次の項を参照してください。

- 「イベントしきい値の設定」（P.21-25）では、イベントの表示頻度（発生回数に基づく）を指定するしきい値の設定方法について説明します。各ポリシー内のイベント単位でしきい値を設定できます。
- 「侵入ポリシー単位の抑制の設定」（P.21-30）では、指定されたイベントの通知を各ポリシー内の送信元 IP アドレス単位または宛先 IP アドレス単位で抑制する方法について説明します。

イベントしきい値の設定

ライセンス：Protection

指定された期間内にイベントが生成された回数に基づいて、システムが侵入イベントを記録して表示する回数を制限するための個別のルールのしきい値を侵入ポリシー単位で設定できます。これにより、大量の同じイベントが原因で機能が麻痺するのを避けることができます。しきい値は、共有オブジェクト ルール単位標準テキスト ルール単位、またはプリプロセッサ ルール単位で設定できます。

詳細については、次の項を参照してください。

- 「イベントしきい値の設定について」（P.21-26）
- 「侵入イベントしきい値の追加と変更」（P.21-27）
- 「侵入イベントしきい値の表示と削除」（P.21-29）
- 「ルールのしきい値の設定」（P.21-7）

イベントしきい値の設定について

ライセンス：Protection

まず、しきい値タイプを指定する必要があります。次の表に示すオプションの中から選択できます。

表 21-6　しきい値設定オプション

オプション	説明
Limit	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [Limit] に、[Count] を 10 に、[Seconds] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。
Threshold	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [Threshold] に、[Count] を 10 に、[Seconds] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[Seconds] と [Count] のカウンタをリセットします。次の 25 秒間にルールがさらに 10 回トリガーします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。
Both	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [Both] に、[Count] を 2 に、[Seconds] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回トリガーとして使用した場合、しきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される）。

次に、トラッキングを指定する必要があります。これにより、イベントしきい値が送信元 IP アドレス単位と宛先 IP アドレス単位のどちらで計算されるかが決まります。次の表の中から、システムがイベント インスタンスを追跡する方法を指定するためのオプションの 1 つを選択します。

表 21-7　IP しきい値設定オプション

オプション	説明
Source	送信元 IP アドレス単位でイベント インスタンス カウントを計算します。
Destination	宛先 IP アドレス単位でイベント インスタンス カウントを計算します。

最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 21-8　しきい値のインスタンス/時間のオプション

オプション	説明
Count	しきい値を満たすために必要な、追跡する IP アドレス単位で指定された期間単位のイベント インスタンスの数。
Seconds	カウントがリセットされるまでの秒数。しきい値タイプを [limit] に、トラッキングを [Source IP] に、[count] を [10] に、[seconds] を [10] に設定した場合は、システムが指定された送信元ポートから 10 秒間に発生した最初の 10 のイベントを記録して表示します。最初の 10 秒間に 7 つのイベントしか発生しなかった場合は、システムがそれらのイベントを記録して表示します。最初の 10 秒間に 40 のイベントが発生した場合は、システムが 10 のイベントを記録して表示してから 10 秒後にカウントを再開します。

侵入イベントのしきい値設定は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベント抑制のいずれかと組み合わせて使用することもできることに注意してください。詳細については、「動的ルール状態の追加」（P.21-33）、「イベントのフィルタリング」（P.32-94）、および「侵入ポリシー単位の抑制の設定」（P.21-30）を参照してください。

詳細については、次の項を参照してください。

- 「侵入イベントしきい値の追加と変更」（P.21-27）
- 「ルールのしきい値の設定」（P.21-7）
- 「侵入イベントしきい値の表示と削除」（P.21-29）

ヒント　侵入イベントのパケット ビューでしきい値を追加することもできます。詳細については、「イベント情報の表示」（P.18-22）を参照してください。

侵入イベントしきい値の追加と変更

ライセンス：Protection

1 つ以上の特定のルールのしきい値を設定できます。既存のしきい値設定を個別にまたは同時に変更することもできます。それぞれに 1 つずつのしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

しきい値設定の表示方法と削除方法については、「侵入イベントしきい値の表示と削除」（P.21-29）を参照してください。

また、すべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。詳細については、「グローバル ルールしきい値の使用」（P.30-1）を参照してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ヒント　複数の CPU を搭載した管理対象デバイスでグローバルしきい値または個別のしきい値を設定すると、予想より多くのイベントが生成される場合があります。

イベントしきい値を追加または変更する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、「侵入ポリシー変更のコミット」（P.20-9）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Manage Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　しきい値を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、「侵入ポリシー内のルール フィルタ処理について」（P.21-11）および「侵入ポリシー内のルール フィルタの設定」（P.21-21）を参照してください。

ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　しきい値を設定する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　[Event Filtering] > [Threshold] の順に選択します。

[thresholding] ポップアップ ウィンドウが表示されます。

ステップ 7　設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベント インスタンス数に通知を制限する場合は、[Limit] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[Threshold] を選択します。
- 指定されたイベント インスタンス数後に期間あたり 1 回ずつ通知を提供する場合は、[Both] を選択します。

ステップ 8　イベント インスタンスを送信元 IP アドレスと宛先 IP アドレスのどちらで追跡するかを指定するために [Track By] の該当するオプションを選択します。

ステップ 9　[Count] フィールドで、しきい値として使用するイベント インスタンスの数を指定します。

ステップ 10　[Seconds] フィールドで、イベント インスタンスを追跡する期間を表す秒数を指定します。

ステップ 11　[OK] をクリックします。

システムが、しきい値を追加し、[Event Filtering] カラムのルールの横にイベント フィルタ アイコン（  ）を表示します。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がイベント フィルタの数を示します。

ステップ 12　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、「一般的な侵入ポリシー編集操作」の表を参照してください。

侵入イベントしきい値の表示と削除

ライセンス：Protection

既存のしきい値設定を表示または削除することができます。[Rules Details] ビューを使用してしきい値の既存の設定を表示することによって、それらがシステムに適切かどうかを確認できます。そうでない場合は、新しいしきい値を追加して既存の値を上書きすることができます。

すべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできることに注意してください。詳細については、「グローバル ルールしきい値の使用」（P.30-1）を参照してください。

しきい値を表示または削除する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、「侵入ポリシー変更のコミット」（P.20-9）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Manage Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　表示または削除する、しきい値が設定されたルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、「侵入ポリシー内のルール フィルタ処理について」（P.21-11）および「侵入ポリシー内のルール フィルタの設定」（P.21-21）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　表示または削除する、しきい値が設定された 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　選択したルールのしきい値を削除するには、[Event Filtering] > [Remove Thresholds] の順に選択します。表示される確認のポップアップ ウィンドウで [OK] をクリックします。

ヒント　特定のしきい値を削除するために、ルールを強調表示して、[Show Details] をクリックすることもできます。しきい値設定を展開して、しきい値設定の横にある [Delete] をクリックします。[OK] をクリックして、設定の削除を確認します。

ページが更新され、しきい値が削除されます。

ステップ 7　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、「一般的な侵入ポリシー編集操作」の表を参照してください。

侵入ポリシー単位の抑制の設定

ライセンス：Protection

特定の IP アドレスまたは IP アドレス の範囲が特定のルールまたはプリプロセッサをトリガーしたときの侵入イベント通知を抑制できます。これは、誤検出を回避するのに役立ちます。たとえば、特定の悪用のように見えるパケットを伝送しているメール サーバが存在する場合は、そのメール サーバによってトリガーとして使用されたイベントに関するイベント通知を抑制できます。ルールはすべてのパケットに対してトリガーとして使用されますが、本物の攻撃に対するイベントだけが表示されます。

侵入イベント抑制は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベントしきい値のいずれかと組み合わせて使用することもできることに注意してください。詳細については、「動的ルール状態の追加」（P.21-33）、「イベントのフィルタリング」（P.32-94）、および「イベントしきい値の設定」（P.21-25）を参照してください。

詳細については、次の項を参照してください。

- 「侵入イベントの抑制」（P.21-30）
- 「抑制条件の表示と削除」（P.21-32）

ヒント　侵入イベントのパケット ビューで抑制を追加することもできます。詳細については、「イベント情報の表示」（P.18-22）を参照してください。また、ルール エディタ ページと侵入イベント ページ（イベントが侵入ルールによってトリガーとして使用された場合）の右クリック コンテキスト メニューを使用して、抑制設定にアクセスすることもできます。

侵入イベントの抑制

ライセンス：Protection

ルールに関する侵入イベント通知を抑制できます。ルールに関する通知が抑制されると、ルールはトリガーとして使用されますが、イベントは生成されません。ルールの 1 つまたは複数の抑制を設定できます。リスト内の最初の抑制に最も高いプライオリティが割り当てられます。2 つの抑制が競合している場合は、最初の抑制のアクションが実行されることに注意してください。

無効な値を入力するとフィールドに復元アイコン（  ）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

イベント表示を抑制する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、「侵入ポリシー変更のコミット」（P.20-9）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Manage Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　抑制を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、「侵入ポリシー内のルール フィルタ処理について」（P.21-11）および「侵入ポリシー内のルール フィルタの設定」（P.21-21）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　抑制条件を設定する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　[Event Filtering] > [Suppression] の順に選択します。

[suppression] ポップアップ ウィンドウが表示されます。

ステップ 7　次の [Suppression Type] オプションのいずれかを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[Rule] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[Source] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[Destination] を選択します。

ステップ 8　抑制タイプとして [Source] または [Destination] を選択した場合は、[Network] フィールドに、IP アドレス、アドレス ブロック、または送信元 IP アドレスまたは宛先 IP アドレスとして指定する変数、あるいは、これらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。

FireSIGHT システムで IPv4 CIDR と IPv6 プレフィクス長アドレス ブロックを使用する方法については、「IP アドレスの表記法」（P.1-19）を参照してください。

ステップ 9　[OK] をクリックします。

システムが、抑制条件を追加し、抑制するルールの横にある [Event Filtering] カラムのルールの横にイベント フィルタ アイコン（）を表示します。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がイベント フィルタの数を示します。

ステップ 10　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、「一般的な侵入ポリシー編集操作」の表を参照してください。

抑制条件の表示と削除

ライセンス：Protection

既存の抑制条件を表示または削除することもできます。たとえば、メール サーバが悪用のように見えるパケットを普段から送信しているという理由で、そのメール サーバの IP アドレスから送信されたパケットに関するイベント通知を抑制できます。その後、そのメール サーバが使用停止になり、その IP アドレスが別のホストに再割り当てされたら、その送信元 IP アドレスの抑制条件を削除する必要があります。

定義された抑制条件を表示または削除する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、「侵入ポリシー変更のコミット」（P.20-9）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Manage Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、ページにはルールがメッセージのアルファベット順に一覧表示されます。

ステップ 4　抑制を表示または削除するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、「侵入ポリシー内のルール フィルタ処理について」（P.21-11）および「侵入ポリシー内のルール フィルタの設定」（P.21-21）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　抑制を表示または削除する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　次の 2 つのオプションから選択できます。

- ルールのすべての抑制を削除するには、[Event Filtering] > [Remove Suppressions] を選択します。表示される確認のポップアップ ウィンドウで [OK] をクリックします。
- 特定の抑制設定を削除するには、ルールを強調表示して、[Show Details] をクリックします。抑制設定を展開して、削除する抑制設定の横にある [Delete] をクリックします。[OK] をクリックして、選択した設定の削除を確認します。

ページが更新され、抑制設定が削除されます。

ステップ 7　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、「一般的な侵入ポリシー編集操作」の表を参照してください。

動的ルール状態の追加

ライセンス：Protection

レート ベースの攻撃は、ネットワークまたはホストに過剰なトラフィックを送信することによって、低速化または正規の要求の拒否を引き起こし、ネットワークまたはホストを混乱させようとします。レート ベースの防御を使用して、特定のルールの過剰なルール一致に対応してルール アクションを変更することができます。

詳細については、次の項を参照してください。

- 「動的ルール状態について」（P.21-33）
- 「動的ルール状態の設定」（P.21-34）

動的ルール状態について

ライセンス：Protection

一定期間に多すぎる数のルールの一致が発生した時点を検出するレート ベースのフィルタを含めるように侵入ポリシーを設定できます。インライン展開された管理対象デバイス上でこの機能を使用して、指定された時刻のレート ベースの攻撃をブロックしてから、ルール一致がイベントを生成するだけでトラフィックをドロップしないルール状態に戻すことができます。

レート ベースの攻撃防御は、異常なトラフィック パターンを識別し、正規の要求に対するそのトラフィックの影響を最小限に抑えようとします。特定の宛先 IP アドレスに送信されるトラフィックまたは特定の送信元 IP アドレスから送信されるトラフィックの過剰なルール一致を識別できます。また、検出されたすべてのトラフィックを通して特定のルールの過剰な一致に対処することもできます。

侵入ポリシーでは、侵入ルールまたはプリプロセッサ ルールのレート ベースのフィルタを設定できます。レート ベースのフィルタは次の 3 つの要素で構成されます。

- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率
- レートを超えた時点で実行される新しいアクション（Generate Events、Drop and Generate Events、および Disable の 3 種類がある）
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウトに達すると、レートがしきい値を下回っていれば、ルールのアクションがルールの初期設定に戻ります。

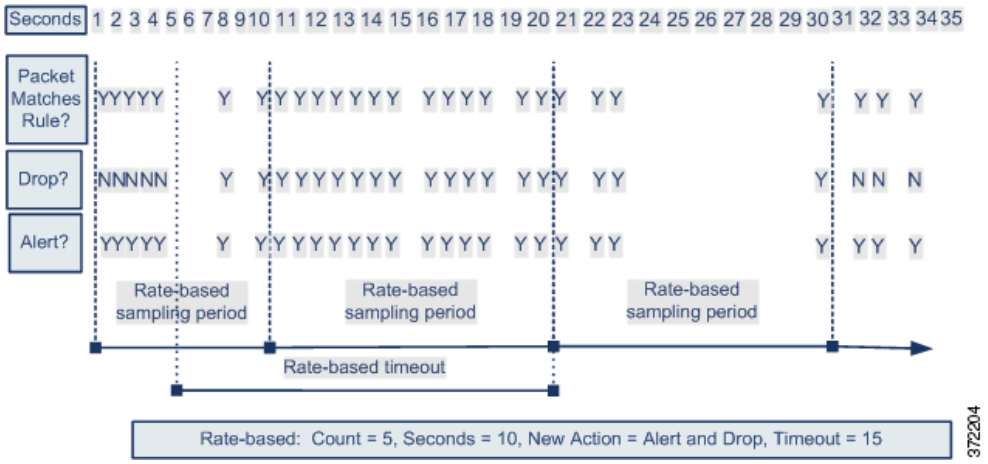
インライン展開のレート ベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レート ベースの設定を使用しない場合、[Generate Events] に設定されたルールはイベントを生成しますが、システムはそのようなルールに関するパケットをドロップしません。ただし、攻撃トラフィックが、レート ベースの基準が設定されたルールと一致した場合は、そのようなルールが最初から [Drop and Generate Events] に設定されていなかったとしても、レート アクションがアクティブな期間にパケットのドロップが実行されます。

注　レート ベースのアクションは、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

同じルールに対して複数のレート ベースのフィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレート ベースのフィルタ アクションが競合している場合は、最初のレート ベースのフィルタのアクションが実行されることに注意してください。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。繰り返しパスワードを特定しようとする試みが、レート ベースの攻撃防御が設定されたルールをトリガーします。レート ベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [Drop and Generate Events] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または過去のサンプリング期間のしきい値を上回っている場合は、新しいアクションが継続されます。新しいアクションは、サンプリング レートがしきい値レートを下回るサンプリング期間の終了後にのみ、[Generate Events] に戻ります。



動的ルール状態の設定

ライセンス：Protection

ルールと一致したすべてのパケットをドロップするのではなく、指定された期間に特定の一致率に達した場合にルールと一致したパケットをドロップするために、ルールを [Drop and Generate Events] 状態に設定しない場合があります。動的ルール状態を使用すれば、ルールのアクションの変更をトリガーするレート、あるレートに達したときに変更すべきアクション、および新しいアクションの継続時間を設定できます。

アクションの変更をトリガーするために特定のヒット数が発生する必要のあるカウントと秒数を指定することによって、そのルールのヒット数を設定します。加えて、タイムアウトが発生したらアクションをルールの以前の状態に戻すタイムアウトを設定できます。

同じルールに対して複数の動的状態フィルタを定義できます。侵入ポリシー内のルール詳細に列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレート ベースのフィルタ アクションが競合している場合は、最初のレート ベースのフィルタのアクションが実行されることに注意してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

注　動的ルール状態は、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

動的ルール状態を追加する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、「侵入ポリシー変更のコミット」（P.20-9）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Rules] をクリックします。

[Rules] ページが表示されます。

ステップ 4　動的ルール状態を追加するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、「侵入ポリシー内のルール フィルタ処理について」（P.21-11）および「侵入ポリシー内のルール フィルタの設定」（P.21-21）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　動的ルール状態を追加する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　[Dynamic State] > [Add Rate-Based Rule State] の順に選択します。

[Add Rate-Based Rule State] ダイアログボックスが表示されます。

ステップ 7　ルール一致の追跡方法を指定するために、該当する [Track By] オプションを選択します。

- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[Source] を選択します。
- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[Destination] を選択します。
- そのルールのすべての一致を追跡する場合は、[Rule] を選択します。

ステップ 8　[Track By] を [Source] または [Destination] に設定した場合は、[Network] フィールドに追跡する各ホストのアドレスを入力します。

単一の IP アドレス、アドレス ブロック、変数、またはこれらの任意の組み合わせで構成されたカンマ区切りのリストを指定できます。FireSIGHT システムで IPv4 CIDR と IPv6 プレフィクス長アドレス ブロックを使用する方法については、「IP アドレスの表記法」（P.1-19）を参照してください。

ステップ 9　攻撃レートを設定する期間あたりのルール一致数を指定します。

- [Count] フィールドで、1 ～ 2147483647 の整数を使用して、しきい値として使用するルール一致の数を指定します。
- [Seconds] フィールドで、1 ～ 2147483647 の整数を使用して、攻撃を追跡する期間を表す秒数を指定します。

ステップ 10　条件が満たされたときに実行すべき新しいアクションを指定する場合は、[New State] オプション ボタンを選択します。

- イベントを生成する場合は、[Generate Events] を選択します。
- インライン展開でイベントを生成し、イベントをトリガーしたパケットをドロップする場合、または、パッシブ展開でイベントを生成する場合は、[Drop and Generate Events] を選択します。
- アクションを実行しない場合は、[Disabled] を選択します。

ステップ 11　[Timeout] フィールドに、新しいアクションを有効にしておく秒数を入力します。タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションのタイムアウトを阻止する場合は、[0] を指定するか、[Timeout] フィールドを空白のままにします。

ステップ 12　[OK] をクリックします。

システムが、動的ルール状態を追加し、[Dynamic State] カラムのルールの横に動的状態アイコン（  ）を表示します。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

必須フィールドを空白にした場合は、フィールドに値を入力する必要があることを伝えるエラー メッセージが表示されます。

ヒント　一連のルールのすべての動的ルール設定を削除するには、[Rules] ページでルールを選択してから、[Dynamic State] > [Remove Rate-Based States] の順に選択します。また、ルールのルール詳細から個別のレート ベースのルール状態フィルタを削除するには、ルールを選択して、[Show Details] をクリックしてから、削除するレート ベースのフィルタのそばにある [Delete] をクリックします。

ステップ 13　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、「一般的な侵入ポリシー編集操作」の表を参照してください。

アラートの追加

ライセンス：Protection

FireSIGHT システムの SNMP アラートを設定する場合は、侵入ポリシー内の特定のルールにアラートを追加できます。詳細については、「SNMP アラートの追加」（P.21-37）。

SNMP アラートの追加

ライセンス：Protection

FireSIGHT システムの SNMP アラートを設定する場合は、トラフィックがルールと一致してイベントが生成されたときにそのアラートを使用するように侵入ポリシー内のルールを設定できます。

SNMP アラートを設定する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、「侵入ポリシー変更のコミット」（P.20-9）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Manage Rules] をクリックします。

[Rules] ページが表示されます。

ステップ 4　SNMP アラートを設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、「侵入ポリシー内のルール フィルタ処理について」（P.21-11）および「侵入ポリシー内のルール フィルタの設定」（P.21-21）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　SNMP アラートを設定する 1 つまたは複数のルールを選択します。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　[Alerting] > [Add SNMP Alert] の順に選択します。

システムが、アラートを追加し、[Alerting] カラムのルールの横にアラート アイコン（）を表示します。ルールに複数のアラート タイプを追加した場合は、アイコン上の数字がアラート タイプの数を示します。

ヒント　ルールから SNMP アラートを削除するには、そのルールの横にあるチェック ボックスをクリックして、[Alerting] > [Remove SNMP Alerts] の順に選択します。

ステップ 7　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、「一般的な侵入ポリシー編集操作」の表を参照してください。

ルール コメントの追加

ライセンス：Protection

ルールにコメントを追加することができます。追加したコメントは、[Rules] ページ上の [Rule Details] ビューで確認できます。

コメントを含む侵入ポリシーの変更をコミットしてから、ルールの [Edit] ページで [Rule Comment] をクリックしてコメントを表示することもできます。ルールの編集方法については、「既存のルールの変更」（P.32-110）を参照してください。

コメントをルールに追加する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、「侵入ポリシー変更のコミット」（P.20-9）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　[Manage Rules] をクリックします。

[Rules] ページが表示されます。

ステップ 4　コメントを追加するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、「侵入ポリシー内のルール フィルタ処理について」（P.21-11）および「侵入ポリシー内のルール フィルタの設定」（P.21-21）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　コメントを追加する 1 つまたは複数のルールを選択します。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6　[Comments] > [Add Rule Comment] の順に選択します。

[Add Comment] ダイアログボックスが表示されます。

ステップ 7　ルール コメントを入力します。

ステップ 8　[OK] をクリックします。

システムが、コメントを追加し、[Comments] カラムのルールの横にコメント アイコン（  ）を表示します。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

ヒント　ルール コメントを削除するには、そのルールを強調表示して、[Show Details] をクリックしてから、ルール コメント セクションで [Delete] をクリックします。侵入ポリシーの変更がコミットされていないコメントがキャッシュされている場合にだけ、コメントを削除できることに注意してください。侵入ポリシーの変更がコミットされた後は、ルール コメントを削除できなくなります。

ステップ 9　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、「一般的な侵入ポリシー編集操作」の表を参照してください。

FireSIGHT ルール状態推奨の管理

ライセンス：FireSIGHT + Protection

FireSIGHT推奨ルール機能を使用して、ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコル（「ネットワーク検出の概要」（P.35-1）を参照）を、それらの資産を保護するために作成されたルールに関連付けることができます。

FireSIGHT推奨ルール機能を設定すると、システムがネットワーク資産に関連付けられた脆弱性から保護するルールの基本ポリシーを検索して、その基本ポリシー内のルールの現在の状態を特定します。その後で、システムは、ルール状態を推奨し、オプションで、次の表内の基準を使用してルールを推奨状態に設定します。

表 21-9　脆弱性に基づく FireSIGHT ルール状態推奨

基本ポリシー ルール状態	ルールは検出された資産を保護するか	推奨ルール状態
Generate Events または Disable	はい	Generate Events
Drop and Generate Events	はい	Drop and Generate Events
任意	いいえ	Disable

シスコ脆弱性調査チーム（VRT）が、シスコから提供されるデフォルト ポリシー内の各ルールに適切な状態を決定します。つまり、基本ポリシーがシスコから提供されるデフォルト ポリシーの場合は、システムでルールを FireSIGHT推奨ルール状態に設定できるようにすることによって、侵入ポリシー内のルールがネットワーク資産に対するシスコの推奨設定と一致します。詳細については、「デフォルト侵入ポリシーの使用」（P.20-18）を参照してください。

ルール状態推奨の生成は、推奨ルール状態を推奨の生成時に使用するのか、後で使用するのかを選択するのと同じぐらい簡単です。高度な推奨オプションを使用すれば、設定をカスタマイズすることができます。

システムは、通常、標準テキスト ルールと共有オブジェクト ルールのルール状態の変更を推奨しますが、プリプロセッサ ルールとデコーダ ルールの変更も推奨できることに注意してください。

侵入ポリシーに最近保存された構成設定に基づいて自動的に推奨を生成するためのタスクをスケジュールできます。推奨ルール状態を生成するためのタスクをスケジュールする方法については、「FireSIGHT 推奨の自動化」（P.49-11）を参照してください。

詳細については、次の項を参照してください。

- 基本ルール状態推奨について
- 高度なルール状態推奨について
- FireSIGHT 推奨の使用

基本ルール状態推奨について

ライセンス：Protection + FireSIGHT

ポリシー内の推奨ルール状態を使用せずに推奨を生成できます。その後で、[Rules] ページの 3 つの絞り込まれたビューのいずれかを使用して、[Generate Events]、[Drop and Generate Events]、または [Disable] に設定するように推奨されているルールを表示できます。これにより、推奨ルール状態を使用した場合に変更されるルールを事前に確認できます。また、推奨を生成してすぐに使用するように選択することもできます。

推奨が絞り込まれた [Rules] ページを表示している最中に、あるいは、ナビゲーション パネルまたは [Policy Information] ページから [Rules] ページに直接アクセスした後で、手動で、ルール状態を設定したり、ルールをソートしたり、ルールの抑制やルールしきい値の設定などの [Rules] ページで使用可能なその他の操作のいずれかを実行したりできます。選択したルールの状態を手動で変更する方法については、「ルール状態の設定」（P.21-22）を参照してください。侵入ポリシー内のルールを調整するための [Rules] ページで使用可能なその他の操作の詳細については、「侵入ポリシー内のルールの管理」（P.21-1）を参照してください。

システムは、手動で設定されたルール状態を変更しません。推奨を生成しながら、推奨ルール状態を使用することにした場合：

- 推奨を生成する前に指定したルールの状態を手動で設定すると、その後、システムはそのルールの状態を変更できなくなる
- 推奨の生成後に指定したルールの状態を手動で設定すると、そのルールの推奨状態が上書きされる

ヒント　ルール状態が推奨状態と異なるルールのリストを侵入ポリシー レポートに含めることができます。詳細については、「侵入ポリシー レポートの表示」（P.20-11）を参照してください。

推奨ルール状態を使用するように選択すると、読み取り専用の FireSIGHT推奨層が侵入ポリシーに追加されますが、後で、推奨ルール状態を使用しないように選択したときに、その階層が削除されることに注意してください。ポリシー層を使用して複数の侵入ポリシーをより効率的に管理する方法については、「侵入ポリシーでのレイヤの使用」（P.23-1）を参照してください。

FireSIGHT推奨ルールの詳細設定を変更せずに推奨を生成する場合は、システムが検出対象のネットワーク全体のすべてのホストのルール状態の変更を推奨することにも注意してください。また、デフォルトで、システムは、オーバーヘッドが低または中のルールに対してのみ推奨を生成し、ルールを無効にする推奨を生成することにも注意してください。詳細については、「高度なルール状態推奨について」（P.21-41）を参照してください。

高度なルール状態推奨について

ライセンス：Protection または Protection + FireSIGHT

詳細設定を使用すれば、システムが脆弱性を監視するネットワーク上のホストを再定義したり、システムがルールのオーバーヘッドに基づいてどのルールを推奨するかに影響を与えたり、ルールを無効にする推奨を生成するかどうかを指定したりできます。

ホスト情報に基づいて特定のパケットのアクティブ ルール処理を動的に適応させる場合は、適応型プロファイルを有効にすることもできます。詳細については、「適応型プロファイルと FireSIGHT推奨ルール」（P.29-3）を参照してください。

詳細については、次の項を参照してください。

- 「検査するネットワークについて」（P.21-41）
- 「ルール オーバーヘッドについて」（P.21-41）

検査するネットワークについて

ライセンス：Protection + FireSIGHT

FireSIGHT推奨ルール機能は、ネットワーク マップ内で検査するネットワークを指定することによって、設定します。その後で、システムが、ネットワークを保護するためにアクティブにすることができるルールを推奨します。ネットワーク マップの詳細については、「ネットワーク マップの使用」（P.36-1）を参照してください。

推奨に対して検査するホストを使用して [Networks] フィールドを設定します。単一 IP アドレスまたはアドレス ブロック、あるいはこのいずれかまたは両方をカンマで区切ったリストを指定できます。

指定したホスト内のアドレスのリストは、否定以外の OR 演算でリンクされ、すべての OR 演算の実行後に AND 演算でリンクされます。

ルール オーバーヘッドについて

ライセンス：Protection

シスコでは、システム パフォーマンスに対するルールの潜在的影響とルールが誤検出を生成する可能性に基づいて、各侵入ルールのオーバーヘッドをなし、低い、中程度、高い、または非常に高いとして格付けしています。[Rules] ページのルール詳細ビューでルールのオーバーヘッド格付けを確認できます。詳細については、「ルール詳細の表示」（P.21-6）を参照してください。

非常に高いを除いて、指定されたオーバーヘッド格付け以下のすべてのルールに基づいて、ルール状態推奨を作成するようにシステムを設定できます。非常に高いオーバーヘッド格付けのルールのルール状態は手動で設定する必要があります。たとえば、中程度オーバーヘッドのルールの推奨を生成すると、システムがなし、低い、または中程度のオーバーヘッド格付けのすべてのルールに基づいて推奨を作成し、高いまたは非常に高いオーバーヘッドのルールの推奨は作成しません。

システムは、イベントを生成する推奨またはイベントをドロップして生成する推奨にルール オーバーヘッドを組み込むことに注意してください。ルールを無効にする推奨にはルール オーバーヘッドを組み込みません。サードパーティの脆弱性にマップされていないローカル ルールにはオーバーヘッドがないことにも注意してください。詳細については、「ローカル ルール ファイルのインポート」（P.53-21）および「サードパーティ製品マッピングの管理」（P.42-33）を参照してください。

特定の設定のオーバーヘッド格付けのルールの推奨を生成した場合でも、別のオーバーヘッドの推奨を生成してから、元のオーバーヘッド設定の推奨を生成し直すことができます。推奨を生成した回数や異なるオーバーヘッド設定の数に関係なく、同じルール セットの推奨を生成するたびに、オーバーヘッド設定ごとに同じルール状態推奨が生成されます。たとえば、オーバーヘッドを中程度に設定してから、高いに設定し、非常に高いに設定してから、もう一度中低度に設定した推奨を生成できます。ネットワーク上のホストとアプリケーションが変更されていなければ、オーバーヘッドが中程度に設定された推奨のセットはいずれも、そのルール セットに対して同じになります。

FireSIGHT 推奨の使用

ライセンス：FireSIGHT + Protection

推奨は、推奨ルール状態の使用の有無と、推奨を生成するための詳細設定の変更の有無に関係なく、生成できます。詳細については、「基本ルール状態推奨について」（P.21-40）および「高度なルール状態推奨について」（P.21-41）を参照してください。

推奨を生成したら、推奨ルール状態を使用できます。また、[Rules] ページで、推奨状態を表示して使用可能な機能を使用することもできます。

FireSIGHT ルール状態推奨を使用する方法：

アクセス：Admin/Intrusion Admin

ステップ 1　[Policies] > [Intrusion] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更が存在する場合は、[OK] をクリックしてそれらの変更を破棄し、次に進みます。別のポリシーでの未保存の変更の保存方法については、「侵入ポリシー変更のコミット」（P.20-9）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3　次の 2 つのオプションから選択できます。

- 推奨を生成しなかった場合は、[No recommendations have been generated. Click here to set up FireSIGHT recommendations] を選択します。
- 推奨を生成した場合は、[Click to change recommendations] を選択します。

[FireSIGHT Recommended Rules Configuration] ページが表示されます。

ステップ 4　次の選択肢があります。

- 対応する侵入ポリシー レポートでルール メッセージ、推奨状態、および実際の状態が推奨状態と異なるすべてのルールの実際の状態を列挙するには、[Include all differences between recommendations and rule states in policy reports] を選択します。詳細については、「侵入ポリシー レポートの表示」（P.20-11）を参照してください。
- デフォルト設定を使用して推奨事項を生成するには、手順に進みます9。
- 高度な推奨オプションを変更するには、ステップ 5 に進みます。

ステップ 5　プラス アイコン（  ）をクリックして [Advanced Settings] セクションを展開します。

高度な FireSIGHT推奨オプションが表示されます。

ステップ 6　[Networks] フィールドで、推奨に対して検査するネットワークを指定します。

FireSIGHT システムで使用する IP アドレス表記については、「IP アドレスの表記法」（P.1-19）を参照してください。

アドレスのリストは、否定以外の OR 演算でリンクされ、すべての OR 演算の実行後に AND 演算でリンクされることに注意してください。詳細については、「検査するネットワークについて」（P.21-41）を参照してください。

ステップ 7　必要に応じて、ルールが、生成する推奨事項に含めなければならない必要があるオーバーヘッドの量を指定するような推奨**しきい値の規則のオーバーヘッドによる）**スライド バーをドラッグします。

スライド バーを右にドラッグすると、より高いオーバーヘッドがルールに含まれ、より多くの推奨が生成されますが、システム パフォーマンスに与える影響も大きくなります。詳細については、「ルール オーバーヘッドについて」（P.21-41）を参照してください。

ステップ 8　次の選択肢があります。

- ルールをディセーブルにする推奨事項を生成するには、[Accept Recommendations to Disable Rules] チェック ボックスをオンにします。

  ルールをディセーブルにする推奨を受け入れると、ルールの適用範囲が制限されることに注意してください。

- ルールをディセーブルにする推奨を生成しない場合は、[Accept Recommendations to Disable Rules] チェック ボックスをオフにします。

  ルールをディセーブルにする推奨を無視すると、ルールの適用範囲が拡大されることに注意してください。

ステップ 9　複数のオプションがあります。

- まだ推奨を生成しておらず、推奨の生成中に、ルール状態が自動的に推奨状態に変更されるようにする場合は、[Generate and Use Recommendations] をクリックします。

  システムが、推奨ルール状態の変更を生成し、自動的にルールを推奨状態に設定します。

- ルール状態を自動的に推奨状態に変更せずにシステムに推奨を生成させる場合は、[Generate Recommendations] をクリックします。

  システムが、推奨ルール状態の変更を生成します。

- 過去に推奨を生成したことがある場合は、[Update Recommendations] をクリックして既存の推奨を更新します。

  システムが、推奨ルール状態の変更を生成し、推奨が使用中の場合は、自動的にルールを推奨状態に設定します。推奨の数、推奨ルール状態変更を伴うホストの数、およびイベントを生成する推奨、イベントをドロップして生成する推奨、またはルールを無効にする推奨の数に関するステータスが更新されます。

- 過去に推奨を生成したことがある場合は、[Use Recommendations] をクリックして、生成したが使用していなかった推奨を使用します。

  システムが、自動的にルールを推奨状態に設定します。

- 推奨を生成してすでに使用している場合は、[Do Not Use Recommendations] をクリックして、現在使用中の推奨の使用を停止します。

  推奨の使用前に特定のルール状態がルールに適用されていなければ、シスシステムが自動的にルールをデフォルトのルール状態にリセットします。この場合は、ルールが特定のルール状態に戻ります。

システムは、Impact Qualification 機能を使用して無効にされた脆弱性に基づく侵入ルールのルール状態を推奨しないことに注意してください。詳細については、「ホスト プロファイルでの脆弱性の使用」（P.37-30）を参照してください。

使用するポリシーを更新する点にも注意してない使用上の推奨事項は、ネットワークおよびルール セットのサイズによって、数分かかることがあります。

注　システムは、常に、ホストにマップされたサードパーティの脆弱性に関連付けられたローカル ルールを有効にするように推奨します。マップされていないローカル ルールに対する状態推奨は生成されません。詳細については、「サードパーティ製品マッピングの管理」（P.42-33）を参照してください。

ステップ 10　オプションで、推奨タイプの横にある [View] をクリックして、[Rules] ページの推奨で絞り込まれたビューに選択した推奨タイプを表示します。

ステップ 11　ポリシーを保存する、編集を継続する、変更を破棄する、またはシステム キャッシュに変更を残したまま終了します。詳細については、「一般的な侵入ポリシー編集操作」の表を参照してください。