侵入ポリシーでのレイヤの使用

多数の管理対象デバイスが存在する大規模な組織では、さまざまな部署や事業部門、場合によっては異なる企業の固有のニーズをサポートするために、多数の侵入ポリシーが存在することがあります。侵入ポリシーのルール設定や詳細設定は、ポリシー *レイヤ*という構成要素に含まれています。このポリシー レイヤを使用することにより、複数のポリシーをより効率的に管理できます。

ポリシーの作成および編集は、レイヤを意識せずに行えます。ポリシーにユーザ レイヤを追加していなければ、ルール設定および詳細設定を変更することができます。システムは単一の設定可能なレイヤに変更を自動的に含めます。必要に応じて、最大 200 までレイヤを追加できます。それらのレイヤでは、ルール設定および詳細設定の組み合わせを自由に設定できます。ユーザ レイヤのコピー、マージ、移動、削除を実行できます。最も重要なこととして、個々のユーザ レイヤを他のポリシーと共有できます。

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 レイヤについて」（P.23-1）では、基本ポリシーを構成するレイヤについて、またそれらの使用方法について説明します。
- 「ユーザ レイヤの設定」（P.23-10）では、ユーザ設定可能なレイヤの追加、コピー、マージ、および共有方法について、またルールと詳細設定に関する設定ページの表示およびアクセス方法について説明します。

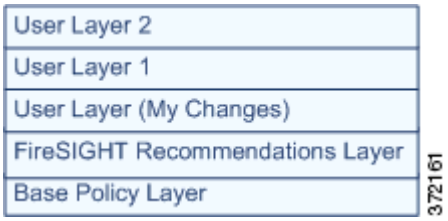
侵入ポリシー レイヤについて

ライセンス：Protection

レイヤを追加していないポリシーには、読み取り専用の基本ポリシーのレイヤと、デフォルトで「My Changes」という名前が付けられているユーザ設定可能な単一のレイヤが含まれます。ネットワーク検出 データに基づくルール状態の推奨を生成して使用する場合、基本ポリシーのすぐ上に読み取り専用の FireSIGHT 推奨レイヤが自動的に挿入されます。ユーザ設定可能なレイヤのコピー、マージ、移動、または削除を実行できます。また、すべてのユーザ設定可能なレイヤを他の侵入ポリシーと共有することができます。My Changes レイヤはユーザ設定可能なレイヤです。

各ポリシー レイヤには、侵入ルール、プリプロセッサ ルール、および詳細設定すべての設定一式が含まれます。スタックの下部のレイヤには、ポリシーの作成時に選択した基本ポリシーのすべての設定が含まれます。ポリシー レイヤ スタックにおける上位レイヤの設定は、下位レイヤの同じ設定よりも優先されます。レイヤで明示的に設定されていない機能は、明示的に設定されている次の高いレイヤから設定を継承します。

次の図は、基本ポリシー レイヤと初期設定の My Changes レイヤに加え、2 つのユーザ設定可能なレイヤと FireSIGHT 推奨レイヤが示された侵入ポリシーのレイヤ スタックの例を示しています。この図では、ユーザが追加したユーザ設定可能な各レイヤは、スタックの最上位のレイヤに配置されていることに注目してください。図の User Layer 2 は、最後に追加され、スタックの最上位にあります。



以下のいずれかを実行する場合、ポリシー内の最上位のレイヤが読み取り専用レイヤであるか、または「レイヤの共有」（P.23-3）で説明されてる共有レイヤであるときに、ユーザ設定可能なレイヤが最上位のレイヤとして侵入ポリシーに自動的に追加されます。

- 侵入ポリシーの [Rules] ページからルール操作（つまり、ルール状態、イベント フィルタリング、動的状態、または警告）を変更する。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。
- 詳細設定の有効化、無効化、または変更を実行する。詳細については、「詳細設定の変更」（P.22-2）を参照してください。

システムによって追加されたレイヤの設定は、新しいレイヤで発生したルールまたは詳細設定の変更を除いてすべて継承されます。

注意すべき点として、最上位のレイヤが共有レイヤである場合、最上位のレイヤが他のポリシーによって共有されるように設定したり、共有レイヤをポリシーに追加したりすると、システムによってレイヤが追加されます。

システムがトラフィックにポリシーを適用する場合、レイヤを *フラット化* します。つまり、各オプションに対して 1 つの設定のみを適用します。たとえば、侵入ポリシーの複数のレイヤ内で同じルールの同じ状態を設定する場合、システムは最上位のレイヤで構成された設定を適用します。

ルール アップデートにポリシーの変更を許可しているかどうかに関わらず、ルール アップデートでの変更は、レイヤで行った変更を上書きしないことに注意してください。これは、ルール アップデートでの変更が、基本ポリシー レイヤのデフォルトを決定する基本ポリシーで行われるためです。変更はより上位のレイヤに加えられ、その変更によって、ルール アップデートがデフォルト ポリシーに加えた変更が上書きされます。詳細については、「ルールの更新とローカル ルール ファイルのインポート」（P.53-16）を参照してください。

ヒント　基本ポリシーのデフォルト設定のみに基づいて侵入ポリシーを作成できます。必要に応じて、ルール状態の推奨を使用することもできます。

ポリシー レイヤの使用に関する詳細については、次のセクションを参照してください。

- 「レイヤの共有」（P.23-3）では、他の侵入ポリシーとのレイヤ設定の共有方法を示す侵入ポリシーの例を示します。
- 「レイヤでのルールの使用」（P.23-4）では、侵入ポリシー レイヤでルールを使用する方法について説明します。

- 「マルチレイヤのルール設定の削除」（P.23-5）では、侵入ポリシーの [Rules] ページを使用して、複数のレイヤからイベント フィルタ、動的状態、およびアラートの設定を削除する方法を示します。
- 「推奨FireSIGHTレイヤの使用」（P.23-7）では、レイヤでルール属性を表示および削除する方法について説明します。
- 「詳細設定でのレイヤの使用」（P.23-8）では、侵入ポリシー レイヤで詳細設定を使用する方法について説明します。

レイヤの共有

ライセンス：Protection

他の侵入ポリシーとユーザ設定可能なレイヤを共有できます。レイヤを共有した後にそのレイヤ内で設定を編集する場合、変更内容を確定すると共有レイヤを使用するすべてのポリシーが更新され、影響を受けるすべてのポリシーのリストが表示されます。作成したポリシーの共有レイヤのみ変更できます。

以下の図には、サイト固有のポリシーのソースとして機能するマスター侵入ポリシーの例が示されています。

図のマスター ポリシーには、Site A と Site B の侵入ポリシーに適用可能な設定を持つ全社的レイヤが含まれます。また、各ポリシーのサイト固有のレイヤも含まれます。たとえば、Site A には監視対象ネットワークに Web サーバがないため、保護したり、HTTP インスペクション プリプロセッサのオーバーヘッドを処理したりする必要はありませんが、両方のサイトで TCP ストリームの前処理が必要になる場合があります。この場合、両方のサイトで共有する全社的レイヤで TCP ストリーム処理を有効にし、Site A で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを無効にして、Site B で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを有効にできます。設定の調整が必要な場合、サイト固有のポリシーのより上位のレイヤで設定を編集することによって、各サイトのポリシーをさらに調整することもできます。

この例のマスター ポリシーでフラット化された設定値そのものがトラフィックを監視するのに役立つ訳ではありませんが、サイト固有のポリシーを設定および更新する際に時間が節約されるため、ポリシーのレイヤで活用することができます。

その他にも多くの高度なレイヤ設定が可能です。たとえば、企業、部門、ネットワーク、さらにはユーザごとにポリシーのレイヤを定義できます。また、1 番目のレイヤにプリプロセッサ設定、2 番目のレイヤにのその他の詳細設定、3 番目のレイヤにルール設定を含めることもできます。

共有レイヤの設定方法については、「ポリシー レイヤの設定操作」の表を参照してください。

ヒント　基本ポリシーが、共有するレイヤが作成されたカスタム ポリシーである場合、侵入ポリシーに共有レイヤを追加することはできません。変更を保存しようとすると、ポリシーに循環依存関係が含まれていることを示すエラー メッセージが表示されます。詳細については、「カスタム基本ポリシーの使用」（P.20-19）を参照してください。

レイヤでのルールの使用

ライセンス：Protection

ユーザ設定可能なすべてのレイヤで、ルールのルール状態、イベント フィルタリング、動的状態、アラート、およびルール コメントを設定できます。変更を加えるレイヤにアクセスした後、そのレイヤの [Rules] ページの設定を、侵入ポリシーの [Rules] ページの設定と同じように追加します。レイヤの [Rules] ページで個々の設定を表示することも、[Rules] ページのポリシー ビューで有効な設定を表示することもできます。[Rules] ページのポリシー ビューのルール設定を変更する場合、ポリシーの最上位のユーザ設定可能なレイヤを変更します。レイヤのドロップダウン リストを使用して、別のレイヤにいつでも切り替えることができます。

次の表では、複数のレイヤで同じ種類の設定を構成した場合の結果について説明しています。

表 23-1　複数のレイヤでのルール設定

設定可能なレイヤ数	設定の種類	目的
1 つ	ルール状態	下位レイヤのルールに対して設定されたルール状態を上書きします。また、下位レイヤで設定されたそのルールのすべてのしきい値、抑制、レートベースのルール状態、およびアラートを無視します。詳細については、「ルール状態の設定」（P.21-22）を参照してください。 基本ポリシーまたは下位レイヤのルールのルール状態を継承したい場合、継承するようにルール状態を設定します。侵入ポリシーの [Rules] ページで作業するときに、継承の状態が [Rule State] 列に表示されない場合は、継承するようにルール状態を設定できないことに注意してください。 特定のレイヤの [Rules] ページで表示する場合に、下位レイヤでルール状態が設定されたルールは黄色で強調表示され、上位レイヤで状態が設定されたルールは赤色で強調表示されることにも注意してください。侵入ポリシーの [Rules] ページはすべてのルール設定の複合ビューであるため、ルール状態は [Rules] ページのポリシー ビューでは色分けされません。
1 つ	しきい値SNMP アラート	下位レイヤのルールの同じ種類の設定を上書きします。しきい値を設定すると、レイヤのルールの既存のしきい値が上書きされることに注意してください。詳細については、「イベントしきい値の設定」（P.21-25）および「アラートの追加」（P.21-36）を参照してください。
1 つ以上	抑制 レートベースのルール状態	選択した各ルールの同じ種類の設定を、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせます。ルール状態が設定されているレイヤより下の設定は無視されます。詳細については、「侵入ポリシー単位の抑制の設定」（P.21-30）および「動的ルール状態の追加」（P.21-33）を参照してください。
1 つ以上	コメント	ルールにコメントを追加します。コメントは、ポリシー固有またはレイヤ固有ではなく、ルール固有です。任意のレイヤの 1 つのルールに 1 つ以上のコメントを追加できます。詳細については、「ルールに関するルール コメントの追加」（P.21-10）を参照してください。

たとえば、あるレイヤでルール状態を [Drop and Generate Events] に設定し、それよりも上位のレイヤで [Disabled] に設定した場合、侵入ポリシーの [Rules] ページには、ルールが無効であることが示されます。

別の例として、あるレイヤでルールの送信元ベースの抑制を 192.168.1.1 に設定し、別のレイヤでそのルールの宛先ベースの抑制を 192.168.1.2 に設定した場合、[Rules] ページには、送信元アドレス 192.168.1.1 と宛先アドレス 192.168.1.2 に関するイベントを抑制する累積的な結果が示されます。抑制およびレートベースのルール状態の設定では、選択した各ルールの同じ種類の設定が、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせられることに注意してください。ルール状態が設定されているレイヤより下の設定は無視されます。

レイヤのビューでルールを変更するには、以下を行います。

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　表示または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。

別のポリシーに保存していない変更がある場合は、[OK] をクリックしてそれらの変更を破棄して続行します。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　ナビゲーション パネルで [Policy Layers] を展開し、表示または編集するポリシー レイヤを展開します。

ステップ 4　表示または編集するポリシー レイヤの下の [Rules] をクリックします。

レイヤの [Rules] ページが表示されます。

表「複数のレイヤでのルール設定」のいずれかの設定を変更できます。

編集可能なレイヤから個々の設定を削除するには、そのレイヤの [Rules] ページでルール メッセージをダブルクリックして、ルールの詳細を表示します。削除する設定の横にある [Delete] をクリックして [OK] を 2 回クリックします。

マルチレイヤのルール設定の削除

ライセンス：Protection

[Rules] ページの侵入ポリシー ビューで 1 つ以上のルールを選択し、ポリシーの複数のレイヤから特定の種類のイベント フィルタ、動的状態、またはアラートを同時に削除できます。

システムは、すべての設定を削除するか、ルール状態がルールに対して設定されているレイヤに遭遇するまで、下位方向にある各レイヤの同じ種類の設定を削除します。ルール状態が設定されているレイヤに遭遇したら、そのレイヤから設定を削除し、それより下のすべてのレイヤは無視します。

共有レイヤまたは基本ポリシーで同じ種類の設定に遭遇したときに、ポリシーの最上位のレイヤが編集可能である場合、システムはそのルールの残りの設定およびルール状態をその編集可能なレイヤにコピーします。そうではない場合、ポリシーの最上位のレイヤが共有レイヤであれば、システムは新しい編集可能なレイヤをその共有レイヤの上に作成し、そのルールの残りの設定およびルール状態をその編集可能なレイヤにコピーします。

注　共有レイヤまたは基本ポリシーからルール設定を削除すると、下位レイヤまたは基本ポリシーにおけるこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーにおける変更を無視しないようにするには、最上位のレイヤでルール状態を [Inherit] に設定します。詳細については、「ルール状態の設定」（P.21-22）を参照してください。

[Rules] ページを使用して複数のレイヤの設定を削除するには、以下を行います。

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　複数の設定を削除する侵入ポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに保存していない変更がある場合は、[OK] をクリックしてそれらの変更を破棄して続行します。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　侵入ポリシーの [Rules] ページにアクセスするには、境界線の上のナビゲーション パネルの上部にある [Rules] をクリックします。

ヒント　また、任意のレイヤの [Rules] ページでレイヤのドロップダウン リストから [Policy] を選択するか、[Policy Information] ページの [Manage Rules] を選択することもできます。

侵入ポリシーの [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　複数の設定を削除するルールを見つけます。次の選択肢があります。

- 現在の表示を並び替えるには、列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、一致するルールがすべて表示されます。

ステップ 5　複数の設定を削除する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。
- 現在のリストのすべてのルールを選択するには、列の一番上にあるチェック ボックスを選択します。

ステップ 6　次の選択肢があります。

- ルールのすべてのしきい値を削除するには、[Event Filtering] > [Remove Thresholds] 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。
- 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。
- ルールのすべてのレートベースのルール状態を削除するには、[Dynamic State] > [Remove Rate-Based Rule States] 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。
- ルールのすべての SNMP アラート設定を削除するには、[Alerting] > [Remove SNMP Alerts] 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。

システムは選択された設定を削除し、ルールの残りの設定をポリシーの最上位の編集可能なレイヤにコピーします。システムが残りの設定をコピーする方法に影響を与える条件については、この手順の概要を参照してください。

注　共有レイヤまたは基本ポリシーからルール設定を削除すると、下位レイヤまたは基本ポリシーにおけるこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーにおける変更を無視しないようにするには、最上位のレイヤでルール状態を [Inherit] に設定します。詳細については、「ルール状態の設定」（P.21-22）を参照してください。

ステップ 7　ポリシーの保存、編集の続行、変更の破棄を行うか、またはシステム キャッシュで変更をそのままにしながら終了します。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。

推奨FireSIGHTレイヤの使用

ライセンス：Protection

ルール状態の推奨を生成した場合、その推奨に基づいてルール状態を自動的に変更するかどうかを選択できます。

推奨されたルール状態を使用することを選択すると、侵入ポリシーの基本レイヤのすぐ上に読み取り専用の組み込み FireSIGHT 推奨システム レイヤが追加または更新されます。それ以後、推奨されたルール状態を使用しないことを選択すると、FireSIGHT 推奨システム レイヤは削除されます。推奨を使用するかしないかを選択することによって、FireSIGHT 推奨レイヤの削除と復元を繰り返すことができますが、レイヤを手動で削除できないことに注意してください。

FireSIGHT 推奨レイヤを追加すると、ナビゲーション パネルの [Policy Layers] の下に FireSIGHT 推奨リンクが追加されます。そのリンクによって、FireSIGHT 推奨レイヤ ページの読み取り専用ビューに誘導されます。FireSIGHT 推奨レイヤ ページから、[Rules] ページの推奨でフィルタリングされたビューを読み取り専用モードで表示できます。[Rules] ページで、さらに読み取り専用の推奨をフィルタリングしたり、列で表示を並び替えたり、個々のルールの詳細を表示したりできます。[Rules] ページでのルールの使用の詳細については、「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。

FireSIGHT 推奨レイヤを追加すると、ナビゲーション パネルの FireSIGHT 推奨リンクの下に [Rules] のサブリンクも追加されます。[Rules] ルのサブリンクによって、FireSIGHT 推奨レイヤの [Rules] ページの読み取り専用画面へのアクセスが提供されます。このビューでは次の点に注意してください。

- 状態列にルール状態のアイコンがない場合、状態は基本ポリシーから継承されます。
- このビューまたは他の [Rules] ページ ビューの FireSIGHT 推奨列にルール状態のアイコンがない場合、このルールに対する推奨は存在しません。

  注意すべき点として、FireSIGHT 推奨レイヤのルールに推奨がない場合、推奨が最後に生成されたときに、そのルールのオーバーヘッド評価は [Recommendation Threshold (By Rule Overhead)] の設定値よりも高くなりました。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。

詳細については、「FireSIGHT ルール状態推奨の管理」（P.21-39）を参照してください。

詳細設定でのレイヤの使用

ライセンス：Protection

ナビゲーション パネルで [Advanced Settings] を選択すると、[Advanced Settings] ページに移動します。このページで侵入ポリシーの詳細設定を有効または無効にしたり、詳細設定の設定ページにアクセスしたりできます。[Advanced Settings] ページでは、侵入ポリシーのすべての詳細設定の有効な状態のサマリが示されます。たとえば、あるレイヤの [SSL Configuration] が [Disabled] に設定され、それより上位のレイヤで [Enabled] に設定されている場合、[Advanced Settings] ページには、[SSL Configuration] が [Enabled] に設定されているように表示されます。[Advanced Settings] ページで加えられる変更は、ポリシーの最上位のレイヤに表示されます。[Advanced Settings] ページでの詳細設定の使用の詳細については、「詳細設定の変更」（P.22-2）を参照してください。

ナビゲーション パネルで [Policy Layers] を展開し、ユーザ設定可能なレイヤのいずれかを選択すると、そのレイヤの [Layer] サマリ ページに移動します。このページで詳細設定を有効または無効にしたり、レイヤの詳細設定の設定ページにアクセスしたりできます。レイヤの名前と説明を変更し、他の侵入ポリシーとレイヤを共有するかどうかを設定できます。詳細については、「レイヤの共有」（P.23-3）を参照してください。

詳細設定についてその状態と設定を基本ポリシーまたは下位レイヤから継承する場合、状態を [Inherit] に設定します。[Advanced Settings] ページで操作するときに、[Inherit] の状態は表示されないことに注意してください。ナビゲーション パネルの [Policy Layers] の下のレイヤの名前を選択することによって、別のレイヤの [Layer] サマリ ページにいつでも切り替えることができます。

詳細設定を有効にすると、詳細設定の設定ページへのサブリンクがナビゲーション パネルのレイヤの名前の下に表示され、詳細設定の設定ページへの [Edit] リンクは、有効にした詳細設定の [Layer] サマリ ページに表示されます。レイヤ内の詳細設定を無効にするか、または [Inherit] に設定すると、詳細設定のサブリンクおよび [Edit] リンクは表示されなくなります。

無効にされている場合はまず有効にしてから、[Edit] をクリックすることによって、[Layer] サマリ ページから詳細設定の設定ページを表示できます。レイヤの詳細設定が有効な場合、ナビゲーション パネルの [Policy Layers] の下にある詳細設定の名前が付いたサブリンクをクリックすることによって、その設定ページを表示できます。

現在のレイヤ、またはそのレイヤの上下のレイヤの詳細設定の状態（有効または無効）を設定できます。レイヤの詳細設定の状態を設定すると、下位レイヤのその詳細設定の状態が上書きされます。あるレイヤで詳細設定が有効な場合、そのレイヤの設定は下位レイヤの詳細設定の構成を上書きします。

別のレイヤで設定された詳細設定の状態は、上位または下位のいずれのレイヤで設定されているかを示すため、色分けされます。[Advanced Settings] ページはすべての状態設定の複合ビューであるため、詳細設定の状態がレイヤの順序で設定されているかどうかを示すために色分けを使用しないことに注意してください。

システムは、設定が有効にされている最上位のレイヤの詳細設定の構成を使用します。設定を明示的に変更しなかった場合は、デフォルト設定が使用されます。たとえば、あるレイヤで DCE/RPC 設定を有効にして変更するものの、それより上位のレイヤで DCE/RPC 設定を有効にして変更しない場合、システムは上位レイヤのデフォルト設定を使用します。

ナビゲーション パネルで [Policy Layers] をクリックすることによって、詳細設定が有効なレイヤ、無効なレイヤ、および継承されたレイヤを表示できます。詳細については、「ユーザ レイヤの設定」（P.23-10）を参照してください。

次の表に、侵入ポリシーのユーザ設定可能なレイヤの [Layer] サマリ ページで実行できる操作を示します。

表 23-2　[Layer] サマリ ページの操作

目的	操作
レイヤの名前または説明の変更	[Name] または [Description] の新しい値を入力します。 この操作は [Advanced Settings] ページでは実行できないことに注意してください。
他の侵入ポリシーとのレイヤの共有	[Allow this layer to be used by other policies] を選択します。 詳細については、「詳細設定でのレイヤの使用」（P.23-8）および「ユーザ レイヤの設定」（P.23-10）を参照してください。 この操作は [Advanced Settings] ページでは実行できないことに注意してください。
現在のレイヤの詳細設定の有効化	有効にする詳細設定の横にある [Enabled] をクリックします。 ページが更新され、詳細設定の設定ページへのサブリンクがナビゲーション パネルのレイヤの名前の下に表示されて、有効にした詳細設定の [Edit] リンクが表示されます。必要に応じて、[Edit] リンクまたは詳細設定のサブリンクをクリックして、現在の設定を変更します。すべての詳細設定の設定ページへのリンクについては、「詳細設定の変更」（P.22-2）を参照してください。 Back Orifice プリプロセッサにユーザ設定可能なオプションがないことに注意してください。
現在のレイヤの詳細設定の無効化	[Disabled] をクリックします。 ページが更新され、詳細設定が有効だった場合、詳細設定のサブリンクと [Edit] が表示されなくなります。
現在のレイヤの下にある最上位のレイヤの設定からの詳細設定の状態および設定の継承	[Inherit] をクリックします。 ページが更新され、詳細設定が有効だった場合、詳細設定のサブリンクと [Edit] が表示されなくなります。

レイヤのビューで詳細設定を表示または変更するには、以下を行います。

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　表示または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。

別のポリシーに保存していない変更がある場合は、[OK] をクリックしてそれらの変更を破棄して続行します。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　ナビゲーション パネルで [Policy Layers] を展開し、表示または編集するレイヤの名前をクリックします。

レイヤの [Layer] サマリ ページが表示されます。

ステップ 4　必要に応じて、表「[Layer] サマリ ページの操作」の操作を実行できます。

ステップ 5　ポリシーの保存、編集の続行、変更の破棄を行うか、またはシステム キャッシュで変更をそのままにしながら終了します。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。

ユーザ レイヤの設定

ライセンス：Protection

[Policy Layers] ページでは、侵入ポリシーのすべてのレイヤの 1 ページのサマリが提供されます。各レイヤについて、スタック内のレイヤまたはそのレイヤの上下のレイヤの詳細設定が有効または無効であるかを表示できます。状態がレイヤで設定されたルールの数、および各ルール状態に設定されたルールの数も表示できます。また、ポリシーのレイヤ全体において有効にされたすべてのルールと詳細設定の実際の効果のサマリを表示することもできます。

このページでは、共有レイヤと非共有レイヤの追加、レイヤ内で編集すためのルールと詳細設定へのアクセス、およびレイヤのコピー、マージ、移動、削除を実行できます。

次の表では、ポリシー レイヤのサマリを表示および解釈する方法が示されています。また、[Policy Layers] サマリ ページで使用可能なレイヤ設定操作についても説明します。

表 23-3　ポリシー レイヤの設定操作

目的	操作
別のポリシーからの共有レイヤの追加	[Add Shared Layer] をクリックし、[Add Shared Layer] ポップアップ ウィンドウのドロップダウン リストから追加するレイヤを選択して、[OK] をクリックします。共有レイヤを追加しない場合は、[Cancel] をクリックします。 [Policy Layers] サマリ ページが表示されます。共有レイヤを選択した場合、画面が更新され、選択した共有レイヤがポリシー内の最上位レイヤとして表示されます。 その他のポリシーに共有レイヤがない場合、ドロップダウン リストは表示されません。ポップアップ ウィンドウで [OK] または [Cancel] をクリックすると、[Policy Layers] サマリ ページに戻ります。
ポリシーへのレイヤの追加	[Add Layer] をクリックします。[Add Layer] ポップアップ ウィンドウでレイヤの一意の名前を入力し、[OK] をクリックするか、レイヤを追加しない場合は、[Cancel] をクリックします。最大 200 階層までレイヤを侵入ポリシーに追加できます。 [Policy Layers] サマリ ページが表示されます。レイヤを追加した場合、画面が更新され、追加したレイヤがポリシー内の最上位レイヤとして表示されます。新規のレイヤでは、詳細設定とルールのすべての状態が、最初は [Inherit] に設定されていて、イベント フィルタリング、動的状態、アラートのルール 操作は何も設定されていないことに注意してください。
他のポリシーとのポリシーの共有の有効化または無効化	ナビゲーション パネルでレイヤの名前をクリックし、[Sharing] チェック ボックスのオン/オフを切り替え、[Back] をクリックして [Policy Layer] サマリ ページに戻ります。 別のポリシーで使用されているレイヤの共有を無効にするには、まずレイヤを他のポリシーから削除するか、他のポリシーを削除しなければならないことに注意してください。
別のレイヤの上または下へのレイヤの移動	レイヤ サマリ内の任意の場所をクリックし、位置矢印（▶）が移動するレイヤの上または下の行を指すまでドラッグします。 画面が更新され、レイヤが新しい場所に表示されます。

表 23-3　ポリシー レイヤの設定操作（続き）

目的	操作
レイヤでのルールの管理または詳細設定の変更	レイヤの編集アイコン（  ）をクリックします。 レイヤの [Layer] サマリ ページが表示されます。このページから、侵入ポリシーの [Rule] ページのレイヤがフィルタリングされたビューの表示、レイヤの詳細設定の有効化、無効化、または継承、およびレイヤの詳細設定の設定ページへのアクセスを行えます。詳細については、「侵入ポリシー内のルールの管理」（P.21-1）および「詳細設定の変更」（P.22-2）を参照してください。 レイヤを追加して新しいレイヤの詳細設定を有効にすると、詳細設定のオプションが、最初は基本ポリシーのデフォルト設定に設定されていることに注意してください。
すぐ下のレイヤとのレイヤのマージ	マージするレイヤのマージ アイコン（  ）をクリックし、プロンプトが表示されたら [OK] をクリックするか、マージを中止する場合は [Cancel] をクリックします。 ページが更新され、レイヤがその下のレイヤとマージされます。 マージされたレイヤは、どちらかのレイヤに固有だったすべての設定を保持します。また、両方のレイヤに同じルールまたは詳細設定の設定が含まれていた場合、上位のレイヤの設定を受け入れます。マージされたレイヤでは、下位レイヤの名前が保持されます。 他のポリシーに追加した共有レイヤを作成したポリシーでは、共有レイヤのすぐ上の非共有レイヤと共有レイヤをマージできますが、共有レイヤをその下の非共有レイヤとマージすることはできません。 別のポリシーに作成した共有レイヤを追加したポリシーでは、共有レイヤをそのすぐ下の非共有レイヤとマージできますが、作成されたレイヤは共有されなくなります。つまり、共有レイヤの上の非共有レイヤを共有レイヤとマージすることはできません。
レイヤのコピー	コピーするレイヤのコピー アイコン（  ）をクリックします。 ページが更新され、レイヤのコピーが最上位のレイヤとして表示されます。共有レイヤをコピーすると、共有されていないコピーが作成されることに注意してください。必要に応じて、他のポリシーと共有可能なレイヤとして識別することができます。
レイヤの削除	削除するレイヤの削除アイコン（  ）をクリックし、プロンプトが表示されたら [OK] をクリックするか、レイヤを削除しない場合は [Cancel] をクリックします。 ページが更新され、レイヤは削除されます。 共有が有効にされたレイヤが別のポリシーで使用されている場合、そのレイヤを削除することはできないことに注意してください。また、共有されていない場合、または共有が許可されていても他の侵入ポリシーに追加されていない場合は、初期設定の My Changes レイヤを削除できることにも注意してください。
[Policy Information] ページの表示	[Policy Summary] をクリックします。 [Policy Information] ページから実行できる操作の説明については、「侵入ポリシーの管理」（P.20-4）を参照してください。

表 23-3　ポリシー レイヤの設定操作（続き）

目的	操作
レイヤの [Layer] サマリ ページの表示	レイヤのサマリでレイヤ名をクリックします。 レイヤの [Layer] サマリ ページが表示されます。 このページからレイヤの名前と説明の変更、他の侵入ポリシーとのレイヤの共有設定、詳細設定の状態の構成、および詳細設定の設定ページへのアクセスを行えます。状態がそのレイヤで設定されたルールのフィルタリングされた [Rules] ページ ビューを表示することもできます。すべてのルールまたはルール状態でフィルタリングされたビューを表示できます。詳細については、「レイヤの共有」（P.23-3）、「詳細設定でのレイヤの使用」（P.23-8）、および「レイヤでのルールの使用」（P.23-4）を参照してください。 または、表示アイコン（🔍）をクリックして共有レイヤの [Layer] サマリ ページにアクセスすることもできます。共有レイヤの [Layer] サマリ ページは読み取り専用であることに注意してください。
基本ポリシーの [Layer] サマリ ページの表示	基本ポリシー サマリの基本ポリシー名をクリックします。 基本ポリシーの [Layer] サマリ ページが表示されます。 このページから侵入ポリシーの別の基本ポリシーを選択したり、インポートされたルールの変更が侵入ポリシーを更新するかどうかを指定したりできます。どの詳細設定が基本ポリシーで有効/無効であるかを表示できます。また、ポリシーの詳細設定のデフォルト設定を表示する読み取り専用設定ページにアクセスできます。ステータス メッセージには、ポリシーで有効にされているルールの数、生成イベントに設定された数やパケットのドロップおよび生成イベントに設定された数が表示されます。このページから、基本ポリシーのすべてのルールの設定を表示する [Rules] ページの読み取り専用ビューにアクセスできます。詳細については、「基本ポリシーについて」（P.20-17）、「ルール更新による基本ポリシーの変更の許可」（P.20-19）、「詳細設定でのレイヤの使用」（P.23-8）、および「レイヤでのルールの使用」（P.23-4）を参照してください。
レイヤレベルの詳細設定の設定ページの表示	レイヤのサマリで詳細設定の名前をクリックします。 基本ポリシーと共有レイヤでは、設定ページが読み取り専用であることに注意してください。詳細については、「レイヤの共有」（P.23-3）および「基本ポリシーについて」（P.20-17）を参照してください。
ルール状態の種類別でのレイヤのルールの表示	レイヤのサマリでドロップおよび生成イベント（✖）、生成イベント（➡）、または無効（➡）のアイコンをクリックするか、表示するルール状態の種類のアイコンの横にある説明をクリックします。 基本ポリシーまたは [Policy Summary] で無効にされたルールは表示されないことに注意してください。各レイヤのサマリでは、レイヤで有効にされたルールの合計数（つまり、生成イベントまたはドロップおよび生成イベントに設定された合計数）および有効にされたルール状態のそれぞれの合計数が提供されます。また、基本ポリシーのルール状態の合計は、ポリシーのデフォルトで有効にされたルール状態の設定であり、[Policy Summary] の合計は、ポリシーのすべてのレイヤの有効にされたすべてのルール状態の有効合計数であることにも注意してください。

侵入ポリシーのレイヤを設定するには、以下を行います。

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。

別のポリシーに保存していない変更がある場合は、[OK] をクリックしてそれらの変更を破棄して続行します。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　ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] サマリ ページが表示され、各レイヤのルール状態と詳細設定のサマリが示されます。また、すべてのレイヤの状態の実際の効果を示すポリシーのフラット化されたビューが表示されます。

各レイヤのサマリにある詳細設定の名前は、以下のように、詳細設定がレイヤで有効、無効、上書き、継承されているかが示されます。

詳細設定の状態	詳細設定の名前の表示方法
レイヤで有効	プレーン テキストで表示
レイヤで無効	取り消し線が引かれる
上位レイヤの設定によって上書きされる	イタリック テキストで表示
下位レイヤから継承される	表示されない

ステップ 4　必要に応じて、表「ポリシー レイヤの設定操作」の操作を実行できます。

ステップ 5　ポリシーの保存、編集の続行、変更の破棄を行うか、またはシステム キャッシュで変更をそのままにしながら終了します。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。