ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用

多数の ASA FirePOWER モジュール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およびネットワーク分析ポリシーが存在することがあります。両方のポリシー タイプでの設定は *レイヤ*と呼ばれる構成要素に含まれており、それを使用することで効率的に複数のポリシーを管理することができます。

侵入ポリシーおよびネットワーク分析ポリシーのレイヤは、原則的に同じ方法で動作します。ポリシー タイプの作成および編集は、レイヤを意識せずに行えます。ポリシー設定を変更でき、ポリシーにユーザ レイヤを追加していない場合は、システムによって自動的に変更内容が単一の設定可能なレイヤ（最初は *My Changes* という名前が付けられています）に含められます。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、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 レイヤを同じタイプの他のポリシーと共有できます。

詳細については、次の各項を参照してください。

- レイヤ スタックについて（19-1 ページ）では、基本ポリシーを構成するユーザ設定可能な組み込み型のレイヤについて説明します。
- レイヤの管理（19-6 ページ）では、ポリシー内でレイヤを使用する方法について説明します。

レイヤ スタックについて

ライセンス：Protection

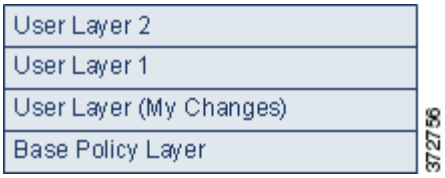
レイヤを追加していないネットワーク分析ポリシーまたは侵入ポリシーには、組み込み型で読み取り専用の基本ポリシー レイヤと、デフォルトで「My Changes」という名前が付けられているユーザ設定可能な単一のレイヤが含まれます。ユーザ設定可能なレイヤのコピー、マージ、移動、または削除を実行できます。また、任意のユーザ設定可能なレイヤを同じタイプの他のポリシーと共有できるように設定できます。

各ポリシー レイヤには、ネットワーク分析ポリシー内のすべてのプリプロセッサまたは侵入ポリシー内のすべての侵入ルールと詳細設定の完全な設定が含まれます。最下部の基本ポリシー 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。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*。

システムはレイヤを *フラット化*します。つまり、ネットワーク トラフィックの処理時にすべての設定の蓄積効果のみを適用します。

ヒント　侵入ポリシーまたはネットワーク分析ポリシーは、基本ポリシーのデフォルト設定に基づいてのみ作成できます。

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 *User Layer 1* と *User Layer 2* が示されたレイヤ 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。



複数のレイヤを使用する場合は、次の点に注意してください。

- 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、またはポリシー間のレイヤの共有（19-10 ページ）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 [ルール（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、ルールを使用した侵入ポリシーの調整（27-1 ページ）を参照してください。
  - プリプロセッサ、侵入ルール、または詳細設定の有効化、無効化、または変更を実行する。

  システムによって追加されたレイヤのすべての設定は、新しいレイヤで発生した変更を除いてすべて継承されます。
- 最上位レイヤが共有レイヤの場合、次のアクションのいずれかを実行すると、システムはレイヤを追加します。
  - 他のポリシーとの最上位レイヤの共有
  - ポリシーへの共有レイヤの追加
- ルール更新にポリシーの変更を許可しているかどうかに関わらず、ルール更新での変更は、レイヤで行った変更を上書きしません。これは、ルール更新での変更が、基本ポリシー レイヤのデフォルト設定を決定する基本ポリシーで行われるためです。変更は常により上位のレイヤに加えられ、その変更によって、ルール更新が基本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、ルール更新およびローカル ルール ファイルのインポート（46-10 ページ）を参照してください。

詳細については、基本レイヤについて（19-2 ページ）を参照してください。

基本レイヤについて

ライセンス：Protection

侵入ポリシーまたはネットワーク分析ポリシーの基本レイヤ（基本ポリシーとも呼ばれる）は、ポリシーのすべての設定のデフォルト設定を定義し、ポリシーの最下位に位置します。新しいポリシーを作成し、新しいレイヤを追加しないで設定を変更すると、その変更は My Changes レイヤに保存され、基本ポリシーの設定を上書きしますが変更はしません。

詳細については、次の各項を参照してください。

- システムによって提供される基本ポリシーについて（19-3 ページ）
- カスタム基本ポリシーについて（19-3 ページ）
- 基本ポリシーの変更（19-4 ページ）
- ルール更新がシステムによって提供される基本ポリシーを変更することを許可する（19-4 ページ）

システムによって提供される基本ポリシーについて

ライセンス：Protection

シスコでは、ネットワーク分析ポリシーおよび侵入ポリシーのいくつかのペアを、ASA FirePOWER モジュールに付属させて提供しています。システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーを使用して、シスコ 脆弱性調査チーム（VRT）のエクスペリエンスを活用することができます。これらのポリシーでは、VRT は侵入ルールおよびプリプロセッサ ルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。これらのシステムによって提供されるポリシーをそのまま使用したり、カスタム ポリシーのベースとして使用することができます。

システムによって提供されるポリシーをベースとして使用する場合、ルール更新をインポートすると、基本ポリシー内の設定が変更される場合があります。しかし、これらの変更内容をシステムによって提供される基本ポリシーに自動的に反映しないようにカスタム ポリシーを設定できます。これにより、ルール更新のインポートとは関係ないスケジュールで、システムによって提供される基本ポリシーを手動で更新できます。いずれの場合も、ルール更新が基本ポリシーに加えた変更によって My Changes または他のレイヤの設定が変更または上書きされることはありません。詳細については、ルール更新がシステムによって提供される基本ポリシーを変更することを許可する（19-4 ページ）を参照してください。

システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。詳細については、システム付属のポリシーについて（18-8 ページ）を参照してください。

カスタム基本ポリシーについて

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシーでシステムによって提供されるポリシーを基本ポリシーとして使用しない場合は、カスタム ポリシーをベースとして使用できます。カスタム ポリシーの設定を調整することで、トラフィックのインスペクションを最も有効な方法で実行できるようになります。これにより、デバイスのパフォーマンスが向上するだけでなく、生成されたイベントにさらに効果的に対応することも可能になります。

最大 5 つのカスタム ポリシーをチェーンすることができます。5 つのうちの 4 つのポリシーで事前に作成されたポリシーが基本ポリシーとして使用され、5 つ目のポリシーでシステムによって提供されたポリシーをベースとして使用する必要があります。

別のポリシーのベースとして使用するカスタム ポリシーに加えた変更は、ベースとして使用するポリシーのデフォルト設定として自動的に使用されます。また、すべてのポリシーにはポリシー チェーン内の最終的なベースとしてシステムによって提供されるポリシーがあるので、カスタム基本ポリシーを使用していてもルール更新のインポートがポリシーに影響を与える場合があります。チェーン内の最初のカスタム ポリシー（システムによって提供されるポリシーをベースとして使用するポリシー）によってルール更新がその基本ポリシーを変更することが許

可されている場合は、ポリシーが影響を受ける可能性があります。この設定の変更の詳細については、ルール更新がシステムによって提供される基本ポリシーを変更することを許可する（19-4 ページ）を参照してください。

これらの設定に関係なく、基本ポリシーへの変更（ルール更新による変更、または基本ポリシーとして使用するカスタム ポリシーを変更する場合）によって My Changes または他のレイヤの設定が変更または上書きされることはありません。

基本ポリシーの変更

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシーに対し異なる基本ポリシーを選択できます。また、オプションで、上位レイヤの変更に影響を与えることなく、ルール更新がシステムによって提供される基本ポリシーを変更することを許可することができます。

基本ポリシーの変更方法：

手順 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー情報（Policy Information）] をクリックします。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 2　[基本ポリシー（Base Policy）] ドロップダウンリストから基本ポリシーを選択します。

手順 3　オプションで、システムによって提供される基本ポリシーを選択する場合は、[基本ポリシーの管理（Manage Base Policy）] をクリックして、侵入ルールの更新によって基本ポリシーが自動的に変更されるかどうかを指定します。

詳細については、ルール更新がシステムによって提供される基本ポリシーを変更することを許可する（19-4 ページ）を参照してください。

手順 4　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（18-16 ページ）を参照してください。

ルール更新がシステムによって提供される基本ポリシーを変更することを許可する

ライセンス：Protection

インポートするルール更新によって、システムによって提供されるポリシーには、ネットワーク分析プリプロセッサの設定変更、侵入ポリシーの詳細設定の変更、新規および更新済みの侵入ルール、および既存ルールの状態の変更が提供されます。ルール更新では、ルールを削除したり、新しいルール カテゴリとデフォルト変数を提供したりすることもできます。詳細については、ルール更新およびローカル ルール ファイルのインポート（46-10 ページ）を参照してください。

ルール更新は、プリプロセッサ、詳細設定およびルールの変更とともに、システムによって提供されるポリシーを常に変更します。デフォルト変数とルール カテゴリに対する変更はシステム レベルで処理されます。詳細については、システムによって提供される基本ポリシーについて（19-3 ページ）を参照してください。

システムによって提供されるポリシーを基本ポリシーとして使用するときは、ルール更新が基本ポリシー（この場合はシステムによって提供されるポリシーのコピー）を変更することを許可することができます。ルール更新で基本ポリシーの更新を許可する場合は、新しいルール更新によって、基本ポリシーとして使用するシステムによって提供されるポリシーに対する変更と同

じ変更が基本ポリシーにも加えられます。対応する設定を変更しなかった場合は、基本ポリシー内の設定によって、ポリシー内の設定が決定されます。ただし、ルール更新では、ポリシー内で行った変更は上書きされません。

ルール更新で基本ポリシーの更新を許可しない場合は、1 つ以上のルール更新のインポート後に、基本ポリシーを手動で更新できます。

ルール更新では、侵入ポリシー内のルール状態またはルール更新で基本の侵入ポリシーの更新が許可されているかどうかに関係なく、VRT が削除した侵入ルールが常に削除されます。ネットワーク トラフィックに変更を再適用するまで、現在適用されている侵入ポリシー ルールは次のように動作します。

- 無効になっているルールは無効のままになります。
- [イベントを生成する（Generate Events）] に設定されたルールでは、トリガーされたときのイベントの生成が継続されます。
- [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールでは、トリガーされたときのイベントの生成と違反パケットのドロップが継続されます。

次の両方の条件が満たされていない限り、ルール更新でカスタム基本ポリシーは変更されません。

- ルール更新が親ポリシーのシステムによって提供される基本ポリシー（つまり、カスタム基本ポリシーの起源となるポリシー）を変更することを許可している。
- 親の基本ポリシー内の対応する設定が上書きされる親ポリシー内の変更を実施していない。

両方の条件が満たされている場合は、親ポリシーを保存したときに、ルール更新内の変更が子ポリシー（つまり、カスタム基本ポリシーを使用したポリシー）に渡されます。

たとえば、ルール更新で以前に無効になっていた侵入ルールを有効にして、親の侵入ポリシー内のルール状態を変更していない場合は、親ポリシーを保存したときに、変更されたルール状態が基本ポリシーに渡されます。

同様に、ルール更新でデフォルトのプリプロセッサ設定を変更し、親のネットワーク分析ポリシーの設定を変更していない場合は、変更された設定は親ポリシーを保存したときに基本ポリシーに渡されます。

詳細については、基本ポリシーの変更（19-4 ページ）を参照してください。

ルール更新がシステムによって提供される基本ポリシーを変更することを許可する方法：

手順 1　システムによって提供されるポリシーを基本ポリシーとして使用するポリシーの編集時に、ナビゲーション パネルで [ポリシー情報（Policy Information）] をクリックします。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 2　[基本ポリシーの管理（Manage Base Policy）] をクリックします。

[基本ポリシー（Base Policy）] 概要ページが表示されます。

手順 3　[新しいルール更新のインストール時に更新（Update when a new Rule Update is installed）] チェックボックスをオンまたはオフにします。

このチェックボックスをオフにしてポリシーを保存してから、ルール更新をインポートすると、[基本ポリシー（Base Policy）] 概要ページに [今すぐ更新（Update Now）] ボタンが表示され、そのページ上のステータス メッセージが更新されて、ポリシーが期限切れであることが示されます。必要に応じて、[今すぐ更新（Update Now）] をクリックして、最近インポートしたルール更新内の変更で基本ポリシーを更新できます。

手順 4　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（18-16 ページ）を参照してください。

レイヤの管理

ライセンス：Protection

[ポリシー層（Policy Layers）] ページでは、ネットワーク分析ポリシーまたは侵入ポリシーの完全なレイヤ スタックの単一ページの概要を示します。このページでは、共有レイヤおよび非共有レイヤの追加、レイヤのコピー、マージ、移動、および削除、各レイヤの概要ページへのアクセス、各レイヤ内の有効、無効、および上書きされている設定の設定ページへのアクセスを行うことができます。

各レイヤについて、次の情報が表示されます。

- レイヤが組み込み型レイヤ、共有ユーザ レイヤ、または非共有ユーザ レイヤであるかどうか
- どのレイヤに最上位の（つまり効果的な）プリプロセッサまたは詳細設定が含まれているか（機能名別に）
- 侵入ポリシーで、状態がレイヤで設定されている侵入ルールの数、および各ルール状態に設定されているルールの数

各レイヤのサマリーにある機能名は、以下のように、設定がレイヤで有効、無効、上書き、または継承されているかを示します。

機能の状態	機能名
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

このページには、有効なすべてのプリプロセッサ（ネットワーク分析）または詳細設定（侵入）、また侵入ポリシーの場合は侵入ルールの最終的な効果の概要も示されます。

次の表に、[ポリシー層（Policy Layers）] ページで使用できるアクションを示します。

表 19-1　ネットワーク分析レイヤおよび侵入ポリシー レイヤの設定アクション

目的	操作
[ポリシー情報（Policy Information）] ページの表示	[ポリシーの概要（Policy Summary）] をクリックします。 [ポリシー情報（Policy Information）] ページで実行できる操作については、ルールを使用した侵入ポリシーの調整（27-1 ページ）、ネットワーク分析ポリシーの準備（21-1 ページ）、および侵入ポリシーの準備（26-1 ページ）を参照してください。

表 19-1　ネットワーク分析レイヤおよび侵入ポリシー レイヤの設定アクション(続き)

目的	操作
レイヤのサマリ ページの表示	レイヤの行でレイヤ名をクリックするか、またはユーザ レイヤの横にある編集アイコン( )をクリックします。表示アイコン( )をクリックして、共有レイヤの読み取り専用のサマリー ページにアクセスすることもできます。 レイヤのサマリー ページで実行できる操作については、ポリシー間のレイヤの共有(19-10 ページ)、レイヤ内のプリプロセッサと詳細設定の設定(19-15 ページ)、およびレイヤでの侵入ルールの設定(19-11 ページ)を参照してください。
レイヤ レベルのプリプロセッサまたは詳細設定の設定ページへのアクセス	レイヤの行で機能名をクリックします。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、レイヤ内のプリプロセッサと詳細設定の設定(19-15 ページ)を参照してください。
ルール状態のタイプ別にフィルタリングされたレイヤ レベルのルール設定ページへのアクセス	レイヤのサマリーでドロップしてイベントを生成する( )、イベントを生成する( )、または無効( )のアイコンをクリックします。選択したルール状態に設定されているルールがレイヤに含まれていない場合、ルールは表示されません。
ポリシーへのレイヤの追加	レイヤの追加(19-7 ページ)を参照してください。
別のポリシーからの共有レイヤの追加	ポリシー間のレイヤの共有(19-10 ページ)を参照してください。
レイヤの名前または説明の変更	レイヤの名前および説明の変更(19-8 ページ)を参照してください。
レイヤの移動、コピー、または削除	レイヤの移動、コピー、および削除(19-8 ページ)を参照してください。
すぐ下のレイヤとのレイヤのマージ	レイヤのマージ(19-9 ページ)を参照してください。

[ポリシー層(Policy Layers)] ページの使用方法:

手順 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層(Policy Layers)] をクリックします。

[ポリシー層(Policy Layers)] サマリー ページが表示されます。

手順 2　ネットワーク分析レイヤおよび侵入ポリシー レイヤの設定アクションの表にある操作を実行できます。

手順 3　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(18-16 ページ)を参照してください。

レイヤの追加

ライセンス: Protection

最大 200 のレイヤをネットワーク分析ポリシーまたは侵入ポリシーに追加できます。レイヤを追加すると、ポリシーで最上位レイヤとして表示されます。初期状態はすべての機能に対して [継承(Inherit)] で、侵入ポリシーでは、イベントのフィルタリング、動的状態、またはルール アクションのアラートは設定されません。

ネットワーク分析ポリシーまたは侵入ポリシーへのレイヤの追加方法:

手順 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層(Policy Layers)] をクリックします。

[ポリシー層(Policy Layers)] ページが表示されます。

手順 2　[ユーザ レイヤ(User Layers)] の横にあるレイヤの追加アイコン( )をクリックします。

[レイヤの追加(Add Layer)] ポップアップ ウィンドウが表示されます。

手順 3　一意のレイヤの**名前**を入力し、[OK] をクリックします。

新しいレイヤが [ユーザ レイヤ(User Layers)] の下に最上位レイヤとして表示されます。

手順 4　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(18-16 ページ)を参照してください。

レイヤの名前および説明の変更

ライセンス: Protection

ネットワーク分析ポリシーまたは侵入ポリシー内のユーザ設定可能なレイヤの名前を変更できます。また、オプションで、レイヤの編集時に表示される説明を追加または変更できます。

レイヤ名の変更方法および説明の追加/変更方法:

手順 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層(Policy Layers)] をクリックします。

[ポリシー層(Policy Layers)] ページが表示されます。

手順 2　編集するユーザ レイヤの横にある編集アイコン( )をクリックします。

レイヤのサマリー ページが表示されます。

手順 3　次の操作を実行できます。

- レイヤの**名前**を変更します。
- レイヤの**説明**を追加または変更します。

手順 4　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(18-16 ページ)を参照してください。

レイヤの移動、コピー、および削除

ライセンス: Protection

初期の My Changes レイヤを含む、ネットワーク分析ポリシーまたは侵入ポリシー内のユーザ レイヤをコピー、移動、または削除できます。次の考慮事項に注意してください。

- レイヤをコピーすると、そのコピーが最上位レイヤとして表示されます。
- 共有レイヤをコピーすると、非共有コピーが作成されます。そのコピーは、任意で後で他のポリシーと共有できます。

- 共有レイヤは削除できません。共有が有効になっているレイヤで別のポリシーと共有していないものは、共有レイヤではありません。

レイヤのコピー、移動、削除方法:

手順 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層(Policy Layers)] をクリックします。

[ポリシー層(Policy Layers)] ページが表示されます。

手順 2　次の操作を実行できます。

- レイヤをコピーするには、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。
- レイヤを [ユーザ レイヤ(User Layers)] ページ領域内で上下に移動させるには、レイヤ サマリー内の任意の空いている場所をクリックし、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。
- レイヤを削除するには、削除するレイヤの削除アイコン( )をクリックし、[OK] 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。

手順 3　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(18-16 ページ)を参照してください。

レイヤのマージ

ライセンス: Protection

ネットワーク分析ポリシーまたは侵入ポリシー内のユーザ設定可能なレイヤを、その下にある次のユーザ レイヤとマージできます。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プリプロセッサ、侵入ルール、または詳細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する共有レイヤを作成するポリシーでは、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するポリシーでは、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。非共有レイヤをその下の共有レイヤとマージすることはできません。

ユーザ レイヤをその下のユーザ レイヤとマージする方法:

手順 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層(Policy Layers)] をクリックします。

[ポリシー層(Policy Layers)] ページが表示されます。

手順 2　2 つのレイヤの上部にあるマージ アイコン( )をクリックし、[OK] 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。

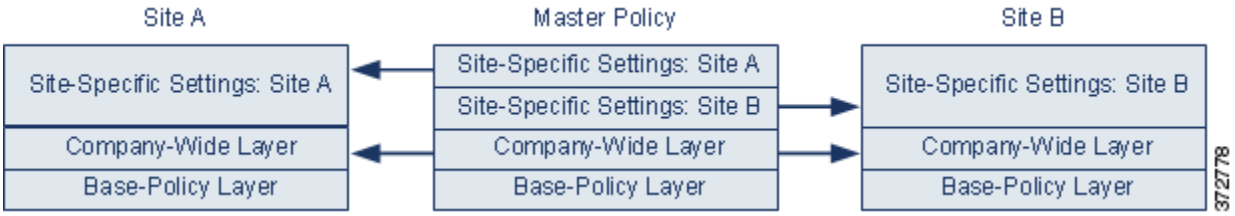
手順 3　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（18-16 ページ）を参照してください。

ポリシー間のレイヤの共有

ライセンス：Protection

ユーザ設定可能なレイヤを同じタイプの他のポリシー（侵入またはネットワーク分析）と共有できます。共有レイヤ内の設定を変更し、変更をコミットすると、共有レイヤを使用するすべてのポリシーが更新され、影響を受けたすべてのポリシーのリストが提供されます。レイヤを作成したポリシー内の共有レイヤ機能の設定のみを変更できます。

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 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、ネットワーク分析ポリシーの場合、Site A にはモニタ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。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。サイト固有のポリシーで上位レイヤの設定を編集することで、必要に応じて、設定の調整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モニタ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、ポリシー層で活用することができます。

その他にも多くのレイヤ設定が可能です。たとえば、ポリシーのレイヤを企業ごと、部門ごと、またはネットワークごとに定義することが可能です。侵入ポリシーの場合は、一方のレイヤに詳細設定を含め、もう一方にルール設定を含めることもできます。

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、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について（19-3 ページ）を参照してください。

他のポリシーとレイヤを共有するには、次の手順を実行する必要があります。

- 共有するレイヤのレイヤ サマリー ページで共有を有効にします。
- 共有するポリシーの [ポリシー層（Policy Layers）] ページで共有レイヤを追加します。

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ことはできません。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する必要があります。

他のポリシーとのレイヤ共有を有効化/無効化する方法:

手順 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層(Policy Layers)] をクリックします。

[ポリシー層(Policy Layers)] ページが表示されます。

手順 2　その他のポリシーと共有するレイヤの横にある編集アイコン( )をクリックします。

レイヤのサマリー ページが表示されます。

手順 3　[共有(Sharing)] チェックボックスをオン(有効)またはオフ(無効)にします。

手順 4　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(18-16 ページ)を参照してください。

ポリシーへの共有レイヤの追加方法:

手順 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層(Policy Layers)] をクリックします。

[ポリシー層(Policy Layers)] ページが表示されます。

手順 2　[ユーザ レイヤ(User Layers)] の横にある共有レイヤの追加アイコン( )をクリックします。

[共有レイヤの追加(Add Shared Layer)] ポップアップ ウィンドウが表示されます。

手順 3　[共有レイヤの追加(Add Shared Layer)] ドロップダウンリストから追加する共有レイヤを選択し、[OK] をクリックします。

[ポリシー層(Policy Layers)] サマリー ページが表示され、選択した共有レイヤがポリシー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 [キャンセル(Cancel)] をクリックすると、[ポリシー層(Policy Layers)] サマリー ページに戻ります。

手順 4　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(18-16 ページ)を参照してください。

レイヤでの侵入ルールの設定

ライセンス: Protection

侵入ポリシーでは、ユーザ設定可能な任意のレイヤで、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 [ルール(Rules)] ページの設定を、侵入ポリシーの [ルール(Rules)] ページの設定と同じように追加します。ルールを使用した侵入ポリシーの調整(27-1 ページ)を参照してください。

レイヤの [ルール(Rules)] ページで個々のレイヤ設定を表示することも、[ルール(Rules)] ページのポリシー ビューですべての設定の最終的な効果を表示することもできます。[ルール(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。[ルール(Rules)] ページにあるレイヤ ドロップダウンリストを使用して、別のレイヤに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 19-2　レイヤ ルールの設定

設定可能なレイヤ数	設定の種類	目的
1	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 (27-22 ページ) を参照してください。 基本ポリシーまたは下位レイヤからルールのルール状態を継承したい場合は、ルール状態を [継承(Inherit)] に設定します。侵入ポリシーの [ルール(Rules)] ページで作業している場合は、ルール状態を [継承(Inherit)] に設定できないことに注意してください。 また、特定のレイヤについてルール状態の設定を [ルール(Rules)] ページで表示すると色分けされて表示されることにも留意してください。有効な状態が下位レイヤで設定されているルールは黄色で強調表示され、有効な状態が上位レイヤで設定されているルールは赤色で強調表示され、有効な状態が現在のレイヤで設定されている場合は強調表示されません。侵入ポリシーの [ルール(Rules)] ページはすべてのルール設定の最終的な効果の複合ビューであるため、ルール状態はこのページでは色分けされません。
1	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(27-25 ページ)」と「SNMP アラートの追加(27-36 ページ)」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、「侵入ポリシーごとの抑制の設定(27-29 ページ)」と「動的ルール状態の追加(27-32 ページ)」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 (27-10 ページ) 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 [ドロップしてイベントを生成する(Drop and Generate Events)] に設定し、それよりも上位のレイヤで [無効(Disabled)] に設定した場合、侵入ポリシーの [ルール(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、[ルール(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。

レイヤでのルールの変更方法:

手順 1　侵入ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] を展開し、変更するポリシー レイヤを展開します。

手順 2　変更するポリシー レイヤのすぐ下にある [ルール（Rules）] をクリックします。

レイヤの [ルール（Rules）] ページが表示されます。

レイヤ ルールの設定の表のいずれかの設定を変更できます。侵入ルールの設定の詳細については、ルールを使用した侵入ポリシーの調整（27-1 ページ）を参照してください。

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 [ルール（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 [削除（Delete）] をクリックして [OK] を 2 回クリックします。

手順 3　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（18-16 ページ）を参照してください。

マルチレイヤ ルール設定の削除

ライセンス: Protection

侵入ポリシーの [ルール（Rules）] ページで 1 つ以上のルールを選択し、侵入ポリシーの複数のレイヤから特定のタイプのイベント 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、設定タイプの削除を停止します。

共有レイヤまたは基本ポリシーで同じタイプ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派生した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から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からの変更を無視しないようにするには、最上位のレイヤのサマリー ページでルール状態を [継承（Inherit）] に設定します。詳細については、ルール状態の設定（27-22 ページ）を参照してください。

複数のレイヤのルール設定を削除する方法:

手順 1　侵入ポリシーの編集中に、ナビゲーション パネルで [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ヒント　また、任意のレイヤの [ルール（Rules）] ページでレイヤのドロップダウン リストから [ポリシー（Policy）] を選択するか、[ポリシー情報（Policy Information）] ページの [ルールの管理（Manage Rules）] を選択することもできます。

侵入ポリシーの [ルール（Rules）] ページが表示されます。

手順 2　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。

ルールの検索については、侵入ポリシー内のルール フィルタリングについて（27-11 ページ）および侵入ポリシー内のルール フィルタの設定（27-21 ページ）を参照してください。

手順 3　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、[イベント フィルタリング（Event Filtering）] > [しきい値の削除（Remove Thresholds）] を選択します。
- ルールのすべての抑制を削除するには、[イベント フィルタリング（Event Filtering）] > [抑制の削除（Remove Suppressions）] を選択します。
- 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、[動的状態（Dynamic State）] > [レート ベースのルール状態の削除（Remove Rate-Based Rule States）] を選択します。
- ルールのすべての SNMP アラート設定を削除するには、[アラート（Alerting）] > [SNMP アラートの削除（Remove SNMP Alerts）] を選択します。

確認のポップアップ ウィンドウが表示されます。

（注）　共有レイヤまたは基本ポリシーから派生した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から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からの変更を無視しないようにするには、最上位のレイヤのサマリー ページでルール状態を [継承（Inherit）] に設定します。詳細については、ルール状態の設定（27-22 ページ）を参照してください。

手順 4　[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。

手順 5　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（18-16 ページ）を参照してください。

カスタム基本ポリシーからのルール変更の受け入れ

ライセンス：Protection

レイヤを追加していないカスタム ネットワーク分析ポリシーまたは侵入ポリシーが別のカスタム ポリシーを基本ポリシーとして使用するとき、以下を行う場合は、そのルール状態を継承するようにルールを設定する必要があります。

- 基本ポリシーのルールに設定されたイベント フィルタ、動的状態、または SNMP アラートを削除する場合
- 基本ポリシーとして使用する他のカスタム ポリシー内のルールに行った後続の変更をルールが受け入れるようにする場合

次の手順では、これを実現する方法について説明します。レイヤを追加したポリシーでこれらのルールの設定を受け入れるには、マルチレイヤ ルール設定の削除（19-13 ページ）を参照してください。

レイヤを追加しなかったポリシー内でのルール変更を受け入れる方法:

手順 1　侵入ポリシーの編集中に、ナビゲーション パネルで [ポリシー層(Policy Layers)] リンクを展開し、[My Changes] リンクを展開します。

手順 2　[My Changes] のすぐ下にある [ルール(Rules)] リンクをクリックします。

My Changes レイヤの [ルール(Rules)] ページが表示されます。

手順 3　設定を受け入れ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。

ルールの検索については、侵入ポリシー内のルール フィルタリングについて(27-11 ページ)および侵入ポリシー内のルール フィルタの設定(27-21 ページ)を参照してください。

手順 4　[ルール状態(Rule State)] ドロップダウンリストから、[継承(Inherit)] を選択します。

手順 5　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(18-16 ページ)を参照してください。

レイヤ内のプリプロセッサと詳細設定の設定

ライセンス: Protection

ネットワーク分析ポリシーでプリプロセッサを設定するときと、侵入ポリシーで詳細詳細を設定するときのメカニズムは同様です。プリプロセッサの有効化および無効化はネットワーク分析の [設定(Settings)] ページで行うことができ、侵入ポリシーの詳細設定の有効化および無効化は侵入ポリシーの [詳細設定(Advanced Settings)] ページで行うことができます。これらのページでは、すべての関連機能の有効な状態の概要も示されます。たとえば、ネットワーク分析 SSL プリプロセッサが、あるレイヤでは無効になっていて上位レイヤでは有効になっている場合、[設定(Settings)] ページにはプリプロセッサが有効であるとして表示されます。これらのページで行った変更は、ポリシーの最上位レイヤに表示されます。

また、プリプロセッサまたは詳細設定を有効化または無効化したり、ユーザ設定可能なレイヤのサマリー ページの設定ページにアクセスしたりできます。このページで、レイヤの名前および説明を変更し、レイヤを同じタイプの他のポリシーと共有するかどうかを設定できます。詳細については、ポリシー間のレイヤの共有(19-10 ページ)を参照してください。ナビゲーション パネルの [ポリシー層(Policy Layers)] の下のレイヤの名前を選択することによって、別のレイヤのサマリー ページに切り替えることができます。

プリプロセッサまたは詳細設定を有効にすると、その機能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、編集アイコン( )がそのレイヤのサマリー ページの機能の横に表示されます。レイヤで機能を無効にしたり、[継承(Inherit)] に設定した場合はこれらは表示されません。

プリプロセッサまたは詳細設定の状態(有効または無効)を設定すると、下位レイヤでのその機能の状態と構成設定が上書きされます。プリプロセッサまたは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 [継承(Inherit)] に設定します。[設定(Settings)] または [詳細設定(Advanced Settings)] ページで操作するときには、[継承(Inherit)] の選択項目は使用できないことに注意してください。

各レイヤのサマリー ページに表示される色分けは、次のように有効な設定が上位レイヤ、下位レイヤ、または現在のレイヤにあることを示します。

- 赤色：有効な設定は上位レイヤにあります
- 黄色：有効な設定は下位レイヤにあります
- 陰影なし：有効な設定は現在のレイヤにあります

[設定（Settings）] および [詳細設定（Advanced Settings）] ページは、関連するすべての設定の複合ビューであるため、これらのページは有効な設定の位置を示すためにカラー コーディングを使用しません。

システムは、機能が有効にされている最上位レイヤの設定を使用します。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、あるレイヤでネットワーク分析 DCE/RPC プリプロセッサを有効にして変更し、それより上位のレイヤでプリプロセッサを有効にするが変更はしない場合、システムは上位レイヤのデフォルト設定を使用します。

次の表に、ユーザ設定可能なレイヤのサマリー ページで実行できる操作を示します。

表 19-3　レイヤのサマリー ページの操作

目的	操作
レイヤの名前または説明の変更	[名前（Name）] または [説明（Description）] の新しい値を入力します。
他の侵入ポリシーとのレイヤの共有	[他のポリシーによるこのレイヤの使用を許可（Allow this layer to be used by other policies）] を選択します。 詳細については、ポリシー間のレイヤの共有（19-10 ページ）を参照してください。
現在のレイヤのプリプロセッサ/詳細設定の有効化または無効化	機能の横にある [有効（Enabled）] または [無効（Disabled）] をクリックします。 有効にすると、設定ページへのサブリンクがナビゲーション パネルのレイヤ名の下に表示され、編集アイコン（  ）が機能の横のサマリー ページに表示されます。 無効にすると、サブリンクと編集アイコンが削除されます。
現在のレイヤの下にある最上位レイヤの設定からのプリプロセッサ/詳細設定の状態および設定の継承	[継承（Inherit）] をクリックします。 ページが更新され、機能を有効にした場合は、ナビゲーション パネルでの機能のサブリンクと編集アイコンは表示されなくなります。
有効なプリプロセッサ/詳細設定の設定ページへのアクセス	現在の設定を変更するには、編集アイコン（  ）または機能のサブリンクをクリックします。 Back Orifice プリプロセッサには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。

ユーザ レイヤのプリプロセッサ/詳細設定を変更する方法：

手順 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] を展開し、変更するレイヤの名前をクリックします。

レイヤのサマリー ページが表示されます。

手順 2　レイヤのサマリー ページの操作の表にある操作を実行できます。

手順 3　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（18-16 ページ）を参照してください。