CHAPTER 33

ネットワーク資産に応じた侵入防御の調整

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（45-1 ページ）を参照）を、侵入ポリシーごとに、資産を保護するために特別に作成されたルールに関連付けることができます。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。FireSIGHT 推奨ルール機能には、FireSIGHT および Protection のライセンスが必要です。

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。その後システムはルール状態を推奨し、オプションで、次の表に示す基準を使用してルールを推奨状態に設定します。

表 33-1　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	検出された資産がルールにより保護されるか	推奨ルール状態
[イベントの生成（Generate Events）] または [無効（Disable）]	はい	[イベントの生成（Generate Events）]
[イベントのドロップおよび生成（Drop and Generate Events）]	はい	[イベントのドロップおよび生成（Drop and Generate Events）]
[任意（any）]	いいえ	[無効（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、システム付属のポリシーについて（23-9 ページ）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ると、設定をさらに調整することができます。推奨ルール状態を使用することを選択すると、読み取り専用の FireSIGHT 推奨レイヤ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ことを選択すると、そのレイヤが削除されるので注意してください。ポリシー レイヤ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、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（24-1 ページ）を参照してください。

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の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（62-11 ページ）を参照してください。

詳細については、次の各項を参照してください。

- 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、[ルール（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、[イベントの生成（Generate Events）]、[イベントのドロップと生成（Drop and Generate Events）]、または [無効化（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 [ルール（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 [ポリシー情報（Policy Information）] ページから [ルール（Rules）] ページに直接アクセスした後に、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（Rules）] ページで可能なその他の操作（ルールの抑制やルールしきい値の設定など）を実行することができます。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（32-23 ページ）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 [ルール（Rules）] ページで使用可能なその他の操作の詳細については、ルールを使用した侵入ポリシーの調整（32-1 ページ）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。推奨の生成中に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、現在の侵入設定のレポートの生成（31-11 ページ）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（33-3 ページ）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（30-3 ページ）を参照してください。

詳細については、次の各項を参照してください。

- 検査するネットワークについて（33-3 ページ）
- ルール オーバーヘッドについて（33-3 ページ）

検査するネットワークについて

ライセンス： Protection + FireSIGHT

FireSIGHT 推奨ルール機能を設定するには、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（48-1 ページ）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 [ネットワーク（Networks）] フィールドを設定します。1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成る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およびルールによる誤検知の可能性に基づいて、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」と格付けしています。[ルール（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（32-5 ページ）を参照してください。

指定し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、ルール状態の推奨を作成するようにシステムを設定できます。たとえば、オーバーヘッドが中程度のルールの推奨を生成する場合は、オーバーヘッド格付けが「なし」、「低い」、または「中程度」のすべてのルールに基づいて推奨が作成され、オーバーヘッドが「高い」または「非常に高い」ルールの推奨は作成されません。

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（66-22 ページ）と サードパーティ製品マッピングの管理（46-34 ページ）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」に設定して推奨を生成し、次に「高い」推奨を生成してから、再び「中低度」の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い場合、オーバーヘッドが「中程度」に設定された両方の推奨は、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（33-2 ページ）と 高度なルール状態推奨について（33-3 ページ）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、[ルール（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

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

手順 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ある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

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

手順 3　以下の 2 つの対処法があります。

- 推奨を生成していない場合は、[推奨が生成されていません。ここをクリックして FireSIGHT 推奨を設定します。（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、[クリックして推奨を変更する（Click to change recommendations）] を選択します。

[FireSIGHT 推奨ルールの設定（FireSIGHT Recommended Rules Configuration）] ページが表示されます。

手順 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、[ポリシー レポートに推奨とルール状態の差異をすべて含める（Include all differences between recommendations and rule states in policy reports）] を選択します。詳細については、現在の侵入設定のレポートの生成（31-11 ページ）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 9 に進みます。
- 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。

手順 5　プラス アイコン（ ）をクリックして [詳細設定（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。

手順 6　[調査するネットワーク（Networks to Examine）] の [ネットワーク（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 アドレスの表記規則（1-24 ページ）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（33-3 ページ）を参照してください。

手順 7　必要に応じて、[FireSIGHT 推奨ルールの設定（FireSIGHT Recommended Rules Configuration）] で、[推奨しきい値（ルール オーバーヘッド別）（Recommendation Threshold (By Rule Overhead)）] スライド バーをドラッグし、生成した推奨事項にルールによって含める必要があるオーバーヘッドの量を指定します。

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（33-3 ページ）を参照してください。

手順 8　次の選択肢があります。

- ルールを無効にする推奨を生成するには、[ルールを無効にする推奨を受け入れる（Accept Recommendations to Disable Rules）] チェックボックスをオンにします。

  ルールを無効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。

- ルールを無効にする推奨を生成しない場合は、[ルールを無効にする推奨を受け入れる（Accept Recommendations to Disable Rules）] チェックボックスをオフにします。

  ルールを無効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。

手順 9　ここでは次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、[推奨を生成して使用する（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。

- システムがルール状態を自動的に推奨状態に変更することなく、推奨を生成するようにする場合は、[推奨を生成する（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。

- 以前に推奨を生成済みの場合は、[推奨を更新する（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、[推奨を使用する（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、[推奨を使用しない（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、脆弱性の Impact Qualification の設定（49-32 ページ）を参照してください。

推奨を使用または使用しないようにポリシーを変更する処理には、ネットワークとルール セットの規模に応じて数分間かかることがある点に注意してください。

（注）　システムでは、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ているローカル ルールを有効化することが常に推奨されます。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（46-34 ページ）を参照してください。

手順 10　（任意）推奨タイプの横にある [表示（View）] をクリックすると、選択した推奨タイプで絞り込まれた推奨が [ルール（Rules）] ページに表示されます。

手順 11　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。