侵入ポリシーでのパフォーマンス設定の使用

シスコには、侵入行為のトラフィックを分析する際のシステムのパフォーマンスを向上するための機能が備わっています。詳細については、次の項を参照してください。

- 「イベント キュー設定」（P.24-1）では、イベント キューで許可されるパケット数を指定し、より大きなストリームに再構築されるパケットのインスペクションを有効または無効にする方法を説明します。
- 「パケット遅延しきい値構成について」（P.24-2）では、デバイスの遅延をパケット遅延しきい値構成の許容レベルで保持する必要性とセキュリティのバランスを実現する方法を説明します。
- 「ルール遅延しきい値構成について」（P.24-6）では、デバイスの遅延をルール遅延しきい値構成の許容レベルで保持する必要性とセキュリティのバランスを実現する方法を説明します。
- 「パフォーマンス統計情報の設定」（P.24-10）では、管理対象デバイスがそのパフォーマンスを監視および報告する動作に関する、基本的なパラメータの設定方法を説明します。
- 「正規表現の制約」（P.24-11）では、PCRE 正規表現のデフォルトの一致および再帰の制限をオーバーライドする方法を説明します。
- 「ルール処理の設定」（P.24-13）では、ルール処理イベント キュー設定を構成する方法を説明します。

イベント キュー設定

ライセンス：Protection

イベント キューで許可されるパケット数を指定し、より大きなストリームに再構築されるパケットのインスペクションを、ストリーム再構成の前後で、有効または無効にすることができます。

イベント キューの設定：

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ある場合は、[OK] をクリックしてそれらの変更を破棄し、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　左側のナビゲーション パネルの [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4　[Performance Settings] の下の [Event Queue Configuration] が有効かどうかにより、次の 2 つの選択肢があります。

- 設定が有効な場合、[Edit] をクリックします。
- 設定が無効の場合、[Enabled] をクリックした後で、[Edit] をクリックします。

[Event Queue Configuration] ページが表示されます。

ページ下部のメッセージは、設定を含む侵入ポリシー層を示します。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。

ステップ 5　次のオプションを修正できます。

- [Maximum Queued Events] フィールドに、キュー内で許可される最大イベント数の値を入力します。
- ストリーム再構成の前後で、より大きなデータ ストリームに再構築されるパケットを検査するには、[Disable content checks that will be inserted through the stream reassembly process] を選択します。再構成の前後の検査はより多くの処理オーバーヘッドを必要とするため、パフォーマンスが低下する可能性があります。
- ストリーム再構成の前後で、より大きなデータ ストリームに再構築されるパケットの検査を無効にするには、[Disable content checks that will be inserted through the stream reassembly process] の選択を解除します。検査を無効にすると、ストリームの検査の処理オーバーヘッドが減少し、パフォーマンスが向上する場合があります。

ステップ 6　ポリシーの保存、編集の続行、変更の破棄、基本ポリシーのデフォルト設定の回復、またはシステム キャッシュ内の変更をそのままにした終了を行います。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。

パケット遅延しきい値構成について

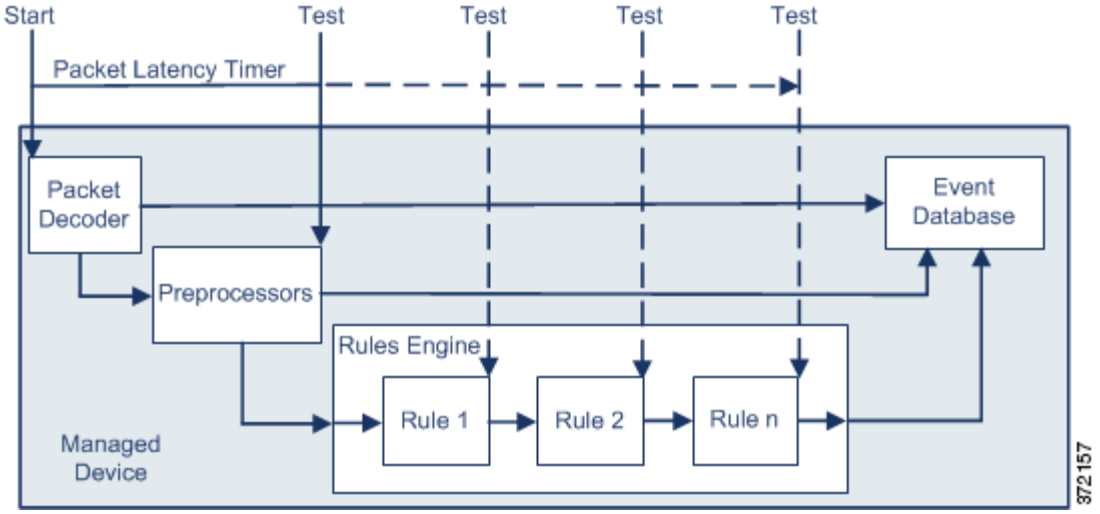
ライセンス：Protection

パケット遅延しきい値構成を有効にすることで、遅延を許容レベルで保持する必要性とセキュリティのバランスを取ることができます。パケット遅延しきい値構成は、該当するデコーダ、プリプロセッサ、およびルールによるパケット処理の総経過時間を測定し、処理時間が設定可能なしきい値を超えるとパケットのインスペクションを終了します。

パケット遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値構成は、厳密なタイミングを強制しないソフトウェア ベースの遅延実装です。

遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。ただし、パケット遅延しきい値構成では、セキュリティと接続性のバランスを取るために使用可能なツールが用意されています。

パケット遅延しきい値構成を有効にすると、デコーダの処理の開始時に各パケットのタイマーが起動します。タイミングは、パケットのすべての処理が終了するか、または処理時間がタイミング テスト ポイントでしきい値を超えるまで継続します。



上の図に示すように、パケット遅延タイミングは次のテスト ポイントでテストされます。

- すべてのデコーダおよびプリプロセッサの処理の完了後、ルールの処理が開始される前
- 各ルールによる処理の後

処理時間がいずれかのテスト ポイントでしきい値を超えると、パケット インスペクションは終了します。

ヒント　パケットの合計処理時間にルーチン TCP ストリームまたは IP フラグメント再構成の時間は含まれません。

パケット遅延しきい値構成は、パケットを処理するデコーダ、プリプロセッサ、またはルールによってトリガーされるイベントに影響を与えません。該当するデコーダ、プリプロセッサ、またはルールは、パケットが完全に処理されるか、または遅延しきい値を超えたためにパケット処理が終了されるか、どちらか先に発生した時点まで通常通りトリガーされます。廃棄ルールがインライン展開の侵入を検知すると、その廃棄ルールがイベントをトリガーし、パケットは廃棄されます。

注　パケット遅延しきい値違反のためにパケットの処理が終了した後は、ルールに対してパケットは評価されません。イベントを引き起こす可能性があったルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

廃棄ルールの詳細については、「ルール状態の設定」（P.21-22）を参照してください。

パケット遅延しきい値構成は、パッシブとインラインの両方の展開でシステムのパフォーマンスを向上することができます。また、過剰な処理時間を必要とするパケットのインスペクションを停止することで、インライン展開の遅延を減らすことができます。これらのパフォーマンスのメリットは、たとえば次の場合に得られる可能性があります。

- パッシブ展開およびインライン展開の両方で、複数のルールによるパケットの順次検査に長時間かかる場合
- インライン展開で、ユーザーが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット処理を遅らせる場合

パッシブ展開では、パケットの処理を停止しても、処理が単に次のパケットに移るだけで、ネットワーク パフォーマンスの回復につながらない可能性があります。

詳細については、次の項を参照してください。

- 「パケット遅延しきい値構成オプションの設定」（P.24-4）
- 「パケットしきい値構成の設定」（P.24-5）

パケット遅延しきい値構成オプションの設定

ライセンス：Protection

次の表に、パケット遅延しきい値構成でユーザが設定できるオプションを示します。

表 24-1　　パケット遅延しきい値構成オプション

オプション	説明
Threshold	パケットのインスペクションが終了する時間をマイクロ秒単位で指定します。推奨される最小しきい値の設定については、「 最小のパケット遅延しきい値設定」の表を参照してください。

ルール 134:3 を有効にして、パケット遅延しきい値を超えたためにシステムがパケットのインスペクションを終了するイベントを生成できます。詳細については、「侵入イベントの表示」（P.18-7）および「ルール状態の設定」（P.21-22）を参照してください。

システム パフォーマンスおよびパケット遅延の測定に影響する要因は、CPU 速度、データ レート、パケット サイズ、プロトコル タイプなど多数あります。このためシスコは、パケット遅延しきい値構成を有効にする場合、ユーザー独自の計算によって特定のネットワーク環境に合った設定を行うまで、次の表のしきい値設定を使用することを推奨します。

表 24-2　　最小のパケット遅延しきい値設定

データ レート	最小しきい値設定（マイクロ秒）
1 Gbps	100
100 Mbps	250
5 Mbps	1000

独自の設定を計算する場合は、次の項目を決定します。

- 1 秒あたりの平均パケット数
- 1 パケットあたりの平均マイクロ秒数

パケット インスペクションを不必要に中断することがないように、ネットワークの 1 パケットあたりの平均マイクロ秒数に重要な安全係数を乗算します。

たとえば、「 最小のパケット遅延しきい値設定」の表では、1 ギガビット環境で 100 マイクロ秒の最小パケット遅延しきい値を推奨しています。この最小推奨値は、1 秒あたり平均 250,000 パケットを示すテスト データに基づいています。これは、1 マイクロ秒あたり 0.25 パケット、言い換えると 1 パケットあたり 4 マイクロ秒に相当します。25 倍すると推奨最小しきい値の 100 マイクロ秒が得られます。

パケットしきい値構成の設定

ライセンス：Protection

パケット遅延しきい値構成の有効化または無効化、および遅延しきい値の変更を行うことができます。

パケット遅延しきい値の設定：

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ある場合は、[OK] をクリックしてそれらの変更を破棄し、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　左側のナビゲーション パネルの [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4　[Performance Settings] の下の [Latency-Based Packet Handling] が有効かどうかにより、次の 2 つの選択肢があります。

- 設定が有効な場合、[Edit] をクリックします。
- 設定が無効の場合、[Enabled] をクリックした後で、[Edit] をクリックします。

[Latency-Based Packet Handling] ページが表示されます。

ページ下部のメッセージは、設定を含む侵入ポリシー層を示します。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。

ステップ 5　推奨される最小しきい値の設定については、「 最小のパケット遅延しきい値設定」の表を参照してください。

ステップ 6　必要に応じて、ページ上部の [Configure Rules for Latency-Based Packet Handling] をクリックして、個々のオプションに関連付けられるルールを表示します。

[Back] をクリックして、[Latency-Based Packet Handling] ページに戻ります。

ステップ 7　ポリシーの保存、編集の続行、変更の破棄、基本ポリシーのデフォルト設定の回復、またはシステム キャッシュ内の変更をそのままにした終了を行います。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。

ルール遅延しきい値構成について

ライセンス：Protection

ルール遅延しきい値構成を有効にすることで、遅延を許容レベルで保持する必要性とセキュリティのバランスを取ることができます。ルール遅延しきい値構成は、各ルールが個々のパケットを処理するための経過時間を測定し、処理時間が設定可能な連続時間数であるルール遅延しきい値を超えた場合に違反ルールおよび関連するルールのグループを一時停止して、一時停止期間が過ぎるとルールを元に戻します。

ルール遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値構成は、厳密なタイミングを強制しないソフトウェア ベースの遅延実装です。

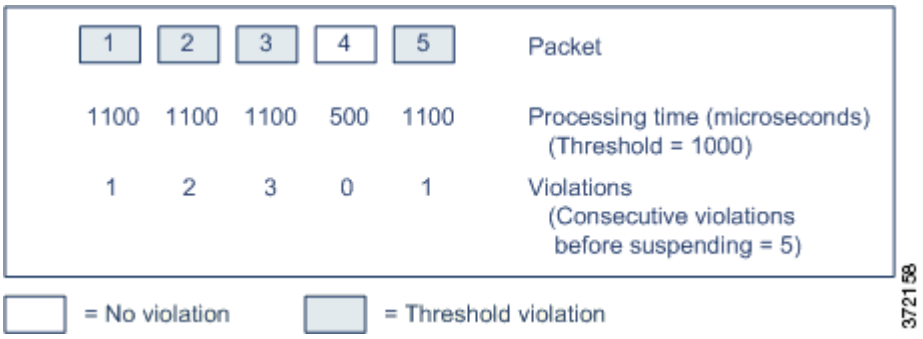
遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。ただし、ルール遅延しきい値構成では、セキュリティと接続性のバランスを取るために使用可能なツールが用意されています。

ルール遅延しきい値構成を有効にすると、パケットがルールのグループに対して処理されるたびに、タイマーが処理時間を測定します。ルール処理時間が指定されたルール遅延しきい値を超えると、システムでカウンタが増加します。連続したしきい値違反の数が指定した数に達すると、システムは次のアクションを実行します。

- 指定された時間、ルールを一時停止する
- ルールが一時停止されたことを示すイベントをトリガーとして使用する
- 一時停止期間が過ぎたらルールを再度有効にする
- ルールが再び有効になったことを示すイベントをトリガーとして使用する

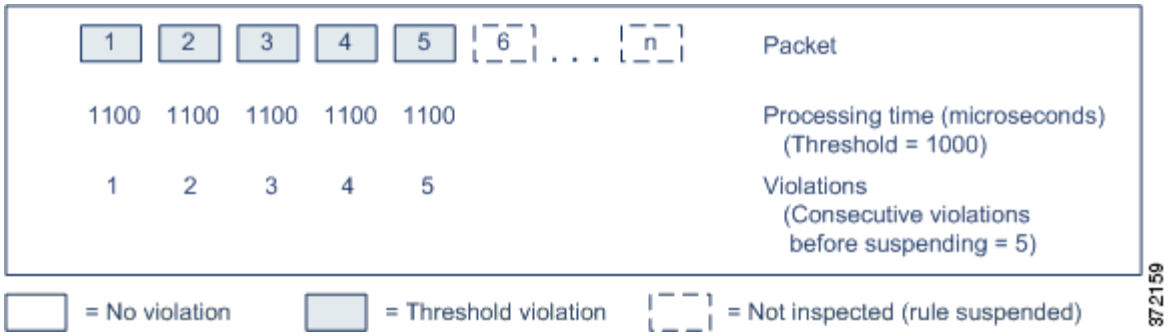
ルールのグループが一時停止しているか、またはルール違反が連続していない場合は、カウンタがゼロになります。ルールを一時停止する前に連続する違反の一部を許可することにより、パフォーマンスへの影響がわずかであると考えられる散発的なルール違反を無視し、繰り返しルール遅延しきい値を超えるルールのより重大な影響に焦点を当てることができます。

次の例は、ルールが一時停止にならない、5 つの連続したルール処理時間を示します。



上の例で、最初の 3 個の各パケットの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反し、違反カウンタは各違反のたびに増加します。4 個目のパケット処理はしきい値に違反しないので、違反カウンタはゼロにリセットされます。5 個目のパケットはしきい値に違反し、違反カウンタは 1 から再開します。

次の例は、ルールが一時停止になる、5 つの連続したルール処理時間を示します。



2 番目の例で、5 個のパケットのそれぞれの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反します。各パケットの 1100 マイクロ秒というルール処理時間が指定された連続する 5 回の違反に対する 1000 マイクロ秒というしきい値に違反するため、ルールのグループは一時停止されます。図中のパケット 6 から n で表される後続のパケットは、一時停止期間が経過するまで、一時停止されたルールに対して検査されません。ルールが再有効化された後にさらにパケットが発生すると、違反カウンタはゼロから再開されます。

ルール遅延しきい値構成は、パケットを処理するルールによってトリガーされる侵入イベントに影響を及ぼしません。ルール処理時間がしきい値を超えるかどうかにかかわらず、パケット内で検出されるすべての侵入に対して、ルールはイベントをトリガーします。侵入を検知するルールがインライン展開の廃棄ルールである場合、パケットは廃棄されます。廃棄ルールがパケット内で侵入を検出し、その結果ルールが一時停止されると、廃棄ルールは侵入イベントをトリガーし、パケットは廃棄され、そのルールと関連するすべてのルールが一時停止されます。廃棄ルールの詳細については、「ルール状態の設定」（P.21-22）を参照してください。

注　パケットは一時停止されたルールに対して評価されません。イベントを引き起こす可能性があった一時停止ルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

ルール遅延しきい値構成は、パッシブとインラインの両方の展開でシステムのパフォーマンスを向上することができます。また、パケットの処理に最も多くの時間を必要とするルールを一時停止することで、インライン展開の遅延を減らすことができます。設定可能な時間が過ぎるまで、パケットは一時停止されたルールに対して再度評価されず、過負荷のデバイスに回復の時間が与えられます。これらのパフォーマンスのメリットは、たとえば次の場合に得られる可能性があります。

- 短期間で作成され、ほとんどテストされていないルールが過剰な処理時間を必要とする場合
- ユーザーが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット インスペクションを遅らせる場合

詳細については、次の項を参照してください。

- 「ルール遅延しきい値構成オプションの設定」（P.24-8）
- 「ルール遅延しきい値構成の設定」（P.24-9）

ルール遅延しきい値構成オプションの設定

ライセンス：Protection

有効な場合、ルールによるパケット処理時間が、[Consecutive Threshold Violations Before Suspending Rule] で指定された回数連続して [Threshold] を超えると、ルール遅延しきい値構成は [Suspension Time] で指定された時間、ルールを一時停止します。

ルール 134:1 を有効にして、ルールが一時停止されるときにイベントを生成できます。また、ルール 134:2 を有効にして、一時停止されたルールが有効化されるときにイベントを生成できます。詳細については、「侵入イベントの表示」（P.18-7）および「ルール状態の設定」（P.21-22）を参照してください。

次の表に、ルール遅延しきい値構成でユーザが設定できるオプションを示します。

表 24-3　ルール遅延しきい値構成オプション

オプション	説明
Threshold	ルールがパケットを検査する際に超えることができない時間をマイクロ秒単位で指定します。。推奨される最小しきい値の設定については、「 最小のルール遅延しきい値設定」の表を参照してください。
Consecutive Threshold Violations Before Suspending Rule	ルールが一時停止される前に、ルールによるパケットの検査時間が [Threshold] で設定された時間を超えることができる、連続した回数を指定します。
Suspension Time	ルールのグループを一時停止する秒数を指定します。

システム パフォーマンスの測定に影響する要因は、CPU 速度、データ レート、パケット サイズ、プロトコル タイプなど多数あります。このためシスコは、ルール遅延しきい値構成を有効にする場合、ユーザー独自の計算によって特定のネットワーク環境に合った設定を行うまで、次の表のしきい値設定を使用することを推奨します。

表 24-4　最小のルール遅延しきい値設定

データ レート	最小しきい値設定（マイクロ秒）
1 Gbps	500
100 Mbps	1250
5 Mbps	5000

独自の設定を計算する場合は、次の項目を決定します。

- 1 秒あたりの平均パケット数
- 1 パケットあたりの平均マイクロ秒数

ルールを不必要に一時停止することがないように、ネットワークの 1 パケットあたりの平均マイクロ秒数に重要な安全係数を乗算します。

ルール遅延しきい値構成の設定

ライセンス：Protection

ルール遅延しきい値構成の有効化または無効化、およびルール遅延しきい値、一時停止されるルールの一時停止時間、ルールを一時停止する前に発生する必要がある連続したしきい値違反の回数の変更を行うことができます。

ルール遅延しきい値の設定：

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ある場合は、[OK] をクリックしてそれらの変更を破棄し、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　左側のナビゲーション パネルの [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4　[Performance Settings] の下の [Latency-Based Rule Handling] が有効かどうかにより、次の 2 つの選択肢があります。

- 設定が有効な場合、[Edit] をクリックします。
- 設定が無効の場合、[Enabled] をクリックした後で、[Edit] をクリックします。

[Latency-Based Rule Handling] ページが表示されます。ページ下部のメッセージは、設定を含む侵入ポリシー層を示します。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。

ステップ 5　推奨される最小しきい値の設定については、「 最小のルール遅延しきい値設定」の表を参照してください。

ステップ 6　必要に応じて、ページ上部の [Configure Rules for Latency-Based Rule Handling] をクリックして、個々のオプションに関連付けられるルールを表示します。

[Back] をクリックして、[Latency-Based Rule Handling] ページに戻ります。

ステップ 7　ポリシーの保存、編集の続行、変更の破棄、基本ポリシーのデフォルト設定の回復、またはシステム キャッシュ内の変更をそのままにした終了を行います。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。

パフォーマンス統計情報の設定

ライセンス：Protection

デバイスがそのパフォーマンスを監視および報告する動作に関する、基本的なパラメータの設定方法を説明します。次の項目を設定することにより、システムがデバイスのパフォーマンス統計情報を更新する間隔を指定できます。

- 秒数
- 分析されるパケット数

注意　サポートにより指示された場合を除き、パフォーマンス統計情報の [Log Session/Protocol Distribution] チェック ボックスが選択された侵入ポリシーを含むアクセス コントロール ポリシーを適用しないでください。

前回パフォーマンス統計情報が更新されてから指定された秒数経過すると、システムは指定された数のパケットが分析されたことを確認します。条件に合う場合、システムはパフォーマンス統計情報を更新します。条件に合わない場合、システムは指定された数のパケットが分析されるまで待機します。

基本的なパフォーマンス統計情報パラメータの設定：

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ある場合は、[OK] をクリックしてそれらの変更を破棄し、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　左側のナビゲーション パネルの [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4　[Performance Settings] の下の [Performance Statistics Configuration] の横にある [Edit] をクリックします。

[Performance Statistics Configuration] ページが表示されます。

ヒント　[Performance Statistics Configuration] の詳細設定を無効にすることはできません。これは、サポートがシステムのトラブルシューティングを行うためです。

ページ下部のメッセージは、設定を含む侵入ポリシー層を示します。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。

ステップ 5　オプションで、任意のパフォーマンス統計情報オプションを変更できます。

- 前回のパフォーマンス統計情報の更新後、分析されたパケット数をカウントするまでにシステムが待機する秒数を指定するには、[Sample time] の値を変更します。
- パフォーマンス統計情報を更新する前に、分析するパケットの数を指定するには、[Minimum number of packets] の値を変更します。

ステップ 6　オプションとして、サポートから依頼があった場合にのみ、トラブルシューティング オプションを変更します。[Troubleshooting Options] の横にある [+] 記号をクリックします。詳細については、「トラブルシューティング オプションについて」（P.22-14）を参照してください。

注意　サポートにより指示された場合を除き、[Log Session/Protocol Distribution] のトラブルシューティング オプションが有効な侵入ポリシーを含むアクセス コントロール ポリシーを適用しないでください。

ステップ 7　ポリシーの保存、編集の続行、変更の破棄、基本ポリシーのデフォルト設定の回復、またはシステム キャッシュ内の変更をそのままにした終了を行います。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。

正規表現の制約

ライセンス：Protection

パケット ペイロードの内容を検査するための侵入ルールで使用される PCRE 正規表現のデフォルトの一致および再帰の制限をオーバーライドできます。侵入ルールにおける PCRE キーワードの使用の詳細については、「PCRE を使用したコンテンツの検索」（P.32-34）を参照してください。デフォルトの制限によってパフォーマンスの最低レベルが確保されます。これらの制限をオーバーライドすると、セキュリティが向上する可能性がありますが、非効率的な正規表現に対してパケット評価を許可することで、パフォーマンスが著しく影響を受ける可能性もあります。

注意　非効率的なパターンの影響に関する知識があり、侵入ルールの作成経験が豊富であるユーザー以外は、デフォルトの PCRE の制限をオーバーライドしないでください。

この機能が無効な侵入ポリシーで、この機能を必要とするルールを有効にする場合、機能を有効にするか、またはポリシーを保存する前に機能が自動的に有効になることを許可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、「詳細設定の自動有効化」（P.22-12）を参照してください。

次の表に、デフォルトの制限をオーバーライドするように設定できるオプションを示します。

表 24-5　正規表現の制約オプション

オプション	説明
Match Limit State	[Match Limit] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [Default] を選択して、[Match Limit] に設定した値を使用する • [Unlimited] を選択して、無制限の数の試行を許可する • [Custom] を選択して、[Match Limit] に対して 1 以上の制限を指定するか、または PCRE の一致の評価を完全に無効化するために 0 を指定する
Match Limit	PCRE 正規表現で定義されたパターンに一致することを試行する回数を指定します。

表 24-5　正規表現の制約オプション（続き）

オプション	説明
Match Recursion Limit State	[Match Recursion Limit] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [Default] を選択して、[Match Recursion Limit] に設定した値を使用する • [Unlimited] を選択して、無制限の数の再帰を許可する • [Custom] を選択して、[Match Recursion Limit] に対して 1 以上の制限を指定するか、または PCRE の再帰を完全に無効化するために 0 を指定する [Match Recursion Limit] が意味を持つためには、[Match Limit] よりも小さい必要があることに注意してください。
Match Recursion Limit	パケット ペイロードに対して PCRE 正規表現を評価する際の再帰数を指定します。

PCRE オーバーライドの設定：

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ある場合は、[OK] をクリックしてそれらの変更を破棄し、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　左側のナビゲーション パネルの [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4　[Performance Settings] の下の [Regular Expression Limits] が有効かどうかにより、次の 2 つの選択肢があります。

- 設定が有効な場合、[Edit] をクリックします。
- 設定が無効の場合、[Enabled] をクリックした後で、[Edit] をクリックします。

[Regular Expression Limits] ページが表示されます。

ページ下部のメッセージは、設定を含む侵入ポリシー層を示します。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。

ステップ 5　「正規表現の制約オプション」の表の任意のオプションを変更できます。

ステップ 6　ポリシーの保存、編集の続行、変更の破棄、基本ポリシーのデフォルト設定の回復、またはシステム キャッシュ内の変更をそのままにした終了を行います。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。

ルール処理の設定

ライセンス：Protection

ルール エンジンがルールに対してトラフィックを評価する場合、特定のパケットまたはパケット ストリームに生成されたイベントをイベント キューに配置し、キュー内の上位のイベントをユーザ インターフェイスに報告します。複数のイベントが発生した場合、ルール エンジンが 1 個のパケットまたはパケット ストリームに対して複数のイベントを記録するように選択できます。これらのイベントのロギングにより、報告されたイベントを超えて情報を収集することができます。このオプションを設定する場合、キュー内に配置可能なイベントの数および記録されるイベントの数を指定できます。また、キュー内のイベントの順序を決定する条件を選択できます。

次の表に、1 個のパケットまたはストリームに対して記録されるイベントの数を決定するために設定できるオプションを示します。

表 24-6　ルール処理設定オプション

オプション	説明
Maximum Queued Events	特定のパケットまたはパケット ストリームに対して保存できるイベントの最大数。
Logged Events	特定のパケットまたはパケット ストリームに対して記録されるイベントの数。これは [Max Events] の値を超えることはできません。
Order Events By	イベント キュー内のイベントの順序を決定するために使用する値。最上位のイベントがユーザ インターフェイスから報告されます。次の中から選択できます。 • priority。イベントの優先順位によってキュー内のイベントを並べ替えます。 • content_length。最も長い識別コンテンツの一致によってイベントを並べ替えます。イベントがコンテンツ長によって並べ替えられる場合、ルール イベントは常にデコーダ イベントおよびプリプロセッサ イベントよりも優先されます。

1 個のパケットまたはストリームに対して記録されるイベント数の設定：

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ある場合は、[OK] をクリックしてそれらの変更を破棄し、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　左側のナビゲーション パネルの [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4　[Performance Settings] の下の [Rule Processing Configuration] が有効かどうかにより、次の 2 つの選択肢があります。

- 設定が有効な場合、[Edit] をクリックします。
- 設定が無効の場合、[Enabled] をクリックした後で、[Edit] をクリックします。

[Rule Processing Configuration] ページが表示されます。ページ下部のメッセージは、設定を含む侵入ポリシー層を示します。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。

ステップ 5　[Rule Processing Configuration] ページの任意のオプションを変更できます。

使用可能な各オプションの詳細については、「ルール処理設定オプション」の表を参照してください。

ステップ 6　ポリシーの保存、編集の続行、変更の破棄、基本ポリシーのデフォルト設定の回復、またはシステム キャッシュ内の変更をそのままにした終了を行います。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。