グローバル ルールしきい値の使用

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しきい値を使用できます。しきい値を設定すると、指定された期間内でルールに一致するトラフィックが特定のアドレスまたはアドレス範囲から送受信される回数に基づいて、システムがイベントを生成します。これにより、多数のイベントでいっぱいなることを回避できます。

イベント通知しきい値は、次の 2 種類の方法で設定できます。

- すべてのトラフィックに対するグローバルしきい値を設定して、指定された期間に特定の送信元または宛先からのイベントが記録され表示される頻度を制限できます。詳細については、「しきい値について」（P.30-1）および「グローバルしきい値の設定」（P.30-3）を参照してください。
- 侵入ポリシー設定での共有オブジェクト ルール、標準テキスト ルール、プリプロセッサ ルールごとにしきい値を設定できます。「イベントしきい値の設定」（P.21-25）を参照してください。

しきい値について

ライセンス：Protection

デフォルトでは、侵入ポリシーごとに、グローバル ルールしきい値が含まれます。デフォルトのしきい値では、各ルールのイベント生成が、同じ宛先に送られるトラフィックで 60 秒あたり 1 つのイベントに制限されます。このグローバルしきい値は、デフォルトですべての侵入ルールとプリプロセッサ ルールに適用されます。しきい値は侵入ポリシーの [Advanced Settings] ページで無効にできることに注意してください。

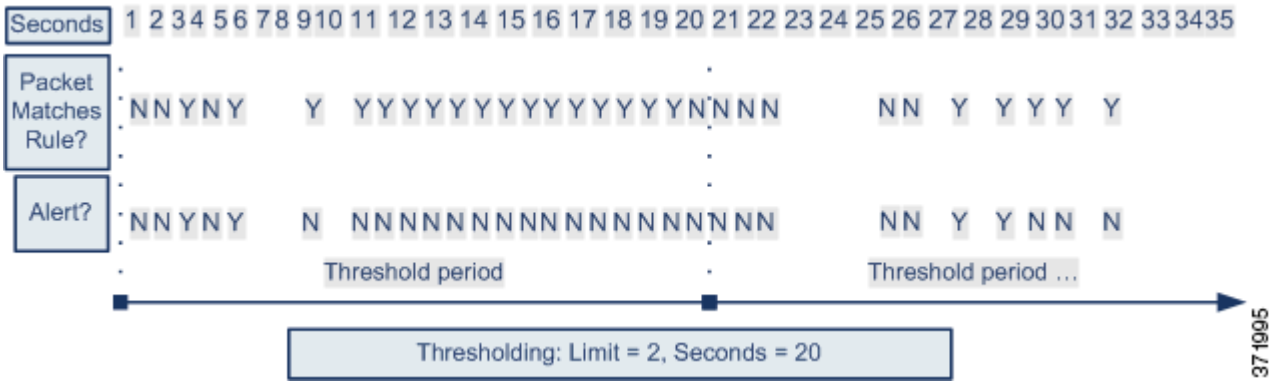
特定のルールで個々のしきい値を設定することにより、このしきい値を上書きすることもできます。たとえば、グローバル制限しきい値を 60 秒ごとに 5 個のイベントに設定してから、SID 1315 について特定のしきい値として 60 秒ごとに 10 個のイベントに設定できます。他のすべてのルールでは 60 秒ごとに 6 個以上のイベントは生成されませんが、SID 1315 では 60 秒ごとに最大 10 個のイベントが生成されます。

ルール ベースのしきい値の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。

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。

次の図は、特定のルールに関して攻撃を受けている例を示します。グローバル制限しきい値では、各ルールのイベント生成が、20 秒あたり 2 つのイベントに制限されます。

期間は 1 秒で始まり 21 秒で終わることに注意してください。期間が終了すると、サイクルが再び開始され、次の 2 つのルール一致によってイベントが生成されます。その後、その期間にさらにイベントが生成されることはありません。



しきい値のオプションについて

ライセンス：Protection

しきい値を使用することにより、期間内で特定の数のイベントのみ生成されるようにするか、またはイベントのセットにつき 1 つのイベントが生成されるようにすることにより、侵入イベントの生成を制限できます。グローバルしきい値を設定する場合、最初にしきい値のタイプを指定します。以下の表を参照してください。

表 30-1　しきい値のオプション

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、33 秒目までにルールが 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 回トリガーされたとします。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 回トリガーされると、しきい値が満たされ、以後のイベントは無視されるため）。

次に、イベント インスタンスの数を、送信元 IP アドレスまたは宛先 IP アドレスのどちらに基づいて計算するかを決定する、トラッキングを指定します。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 30-2　　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、トラッキング IP アドレスまたはアドレス範囲ごとの、指定された期間でのイベント 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] に、[Count] を 10 に、[Seconds] を 10 に設定した場合、特定のソース ポートで 10 秒間に発生した最初の 10 のイベントを記録し表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒間経過してからカウントを再度開始します。

グローバルしきい値の設定

ライセンス：Protection

一定の期間に各ルールによって生成されるイベントの数を管理するために、グローバルしきい値を設定できます。グローバルしきい値を設定すると、特定のしきい値を上書きしない各ルールでそのしきい値が適用されます。しきい値の設定の詳細については、「しきい値について」（P.30-1）を参照してください。

デフォルトでは、グローバルしきい値が設定されます。デフォルト値は次のとおりです。

- **Type** — Limit
- **Track By** — Destination
- **Count** — 1
- **Seconds** — 60

グローバルしきい値の設定方法：

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、「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 パネルで [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　[Intrusion Rule Thresholds] の下の [Global Rule Thresholding] が有効かどうかに応じて、以下の 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。
- 設定が無効である場合、[Enabled] をクリックした後で、[Edit] をクリックします。

[Global Rule Thresholding] 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　[Type] ドロップダウン リストからしきい値のタイプを選択して、秒引数で指定された時間内で以下を行います。

- カウント引数で指定された制限を超えるまで、ルールをトリガーとして使用したパケットごとにイベントを記録して表示する場合、[Limit] を選択します。
- ルールをトリガーとして使用し、カウント引数で設定されたしきい値と同じかその倍数であるインスタンスを表すパケットごとに 1 つのイベントを記録して表示する場合、[Threshold] を選択します。
- カウント引数によって指定された数のパケットがルールをトリガーとして使用した後に 1 つのイベントを記録して表示する場合、[Both] を選択します。

ステップ 6　[Track By] ドロップダウン リストからトラッキング方法を選択します。

- 特定の送信元 IP アドレスからのトラフィックでルールの一致を識別するには、[Source] を選択します。
- 特定の宛先 IP アドレスへのトラフィックでルールの一致を識別するには、[Destination] を選択します。

ステップ 7　次の選択肢があります。

- [Threshold] しきい値の場合、[Count] フィールドのしきい値として使用するルールの一致の数を指定します。
- [Limit] しきい値の場合、[Count] フィールドのしきい値を満たすために必要なトラッキング IP アドレスごとの、指定された期間でのイベント インスタンスの数を指定します。

ステップ 8　次の選択肢があります。

- [Limit] しきい値の場合、攻撃が追跡される期間の秒数を [Seconds] フィールドで指定します。
- [Threshold] しきい値の場合、[Seconds] フィールドで指定した秒数を経過すると、カウントがリセットされます。指定された秒数が経過する前であっても、[Count] フィールドで示されている数のルールが一致すると、カウントはリセットされるのでご注意ください。

ステップ 9　ポリシーの保存、編集の続行、変更の破棄、システム キャッシュ内に変更を残したまま終了のいずれかを行います。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。

グローバルしきい値の無効化

ライセンス：Protection

デフォルトでは、グローバル制限しきい値は、宛先へのトラフィックでのイベントの数を 60 秒あたり 1 個のイベントに制限しています。デフォルトで特定のルールに関するイベントにしきい値を適用し、すべてのルールにしきい値を適用しない場合、最高位のポリシー階層でグローバルしきい値を無効にできます。

グローバルしきい値の無効化：

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、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、「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 パネルで [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　[Intrusion Rule Thresholds] の下の [Global Rule Thresholding] を無効にします。

ステップ 5　ポリシーの保存、編集の続行、変更の破棄、システム キャッシュ内に変更を残したまま終了のいずれかを行います。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。