侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御

侵入ポリシーとファイル ポリシーは FireSIGHT システムの一部として連携して、トラフィックがその宛先に許可される前の最後の防御ラインとして機能します。

- **侵入ポリシー**は、システムの侵入防御機能を制御します。ネットワーク分析ポリシーおよび侵入ポリシーについて（23-1 ページ）を参照してください。
- **ファイル ポリシー**は、システムのネットワークベースのファイル制御および高度なマルウェア防御（AMP）機能を制御します。ファイル ポリシーの概要と作成（37-11 ページ）を参照してください。

ハードウェア ベースの高速パス、セキュリティ インテリジェンス ベースのトラフィック フィルタリング（ブラックリスト登録）、SSL インスペクション ベースの決定、およびトラフィックのデコードと前処理は、ネットワーク トラフィックが侵入、禁止されたファイル、およびマルウェアの有無について検査される**前に**行われます。アクセス コントロール ルールおよびアクセス コントロールのデフォルト アクションによって、侵入ポリシーおよびファイル ポリシーで検査されるトラフィックが決まります。

侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイル ポリシー（またはその両方）を使ってトラフィックを検査するよう、システムに指示できます。

（注） デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイル インスペクションは無効になっています。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。詳細については、トラフィック復号の概要（19-1 ページ）および SSL プリプロセッサの使用（27-77 ページ）を参照してください。

侵入防御および AMP では、次の表に示すように、アクセス コントロール ポリシーのターゲット デバイスで特定のライセンス付与対象の機能を有効にする必要があります。

表 18-1　侵入インスペクションおよびファイル インスペクションのライセンスおよびモデルの要件

機能	説明	ライセンス	サポートされる Defense Center	サポートされるデバイス
侵入防御	侵入およびエクスプロイトを検出し、任意でブロックします	Protection	Any	Any
ファイル制御	ファイル タイプの伝送を検出し、任意でブロックします	Protection	Any	Any
高度なマルウェア防御（AMP）	マルウェアの伝送を検出、保存、追跡し、任意でブロックします キャプチャしたファイルを シスコ クラウドに送信し、マルウェアの分析を行います	Malware	DC500 を除くいずれか	シリーズ 2 と X-シリーズを除くすべて

また、お客様の組織で FireAMP サブスクリプションをご利用の場合、Defense Center は、シスコ クラウドからエンドポイント ベースのマルウェア検出データを受信することもできます。Defense Center は、このデータを、ネットワークベースのファイルおよびシステム生成のマルウェア データとともに提示します。FireAMP データのインポートには、FireAMP サブスクリプションに加えてライセンスは必要ありません。詳細については、FireAMP 用のクラウド接続の操作（37-29 ページ）を参照してください。

侵入、禁止されたファイル、およびマルウェアの有無についてトラフィックを検査する詳細については、以下を参照してください。

- 許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション（18-2 ページ）
- 侵入防御パフォーマンスの調整（18-10 ページ）
- ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整（18-21 ページ）

許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション

ライセンス：Protection または Malware

サポートされるデバイス：機能に応じて異なる

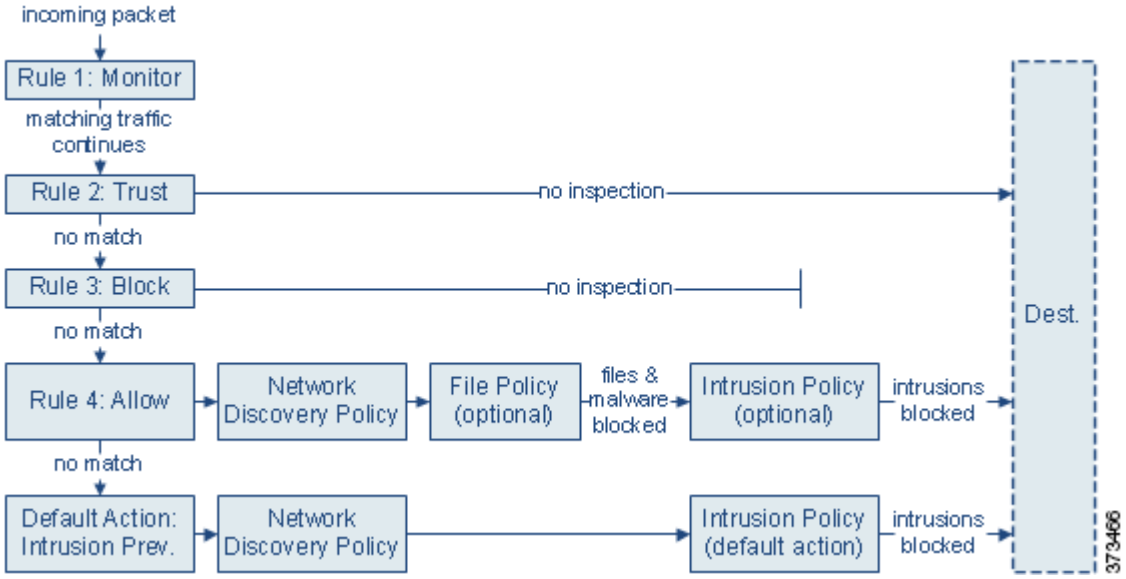
サポートされる防御センター：機能に応じて異なる

侵入ポリシーおよびファイル ポリシーは、トラフィックがその宛先に許可される前の最後の防衛ラインとして、システムの侵入防御、ファイル制御、および AMP 機能を制御します。ハードウェア ベースの高速パス ルール、セキュリティ インテリジェンス ベースのトラフィック フィルタリング、SSL インスペクションの決定（復号を含む）、デコードと前処理、およびアクセス コントロール ルールの選択は、侵入インスペクションおよびファイル インスペクションの**前に**行われます。

アクセス コントロール ルールは、複数の管理対象デバイスでネットワーク トラフィックを処理する詳細な方法を提供します。侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイル ポリシー（またはその両方）を使ってトラフィックを検査するよう、システムに指示できます。アクセス コントロール ルールの条件は単純または複雑にできます。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、およびユーザごとにトラフィックを制御できます。

システムは、指定した順にアクセス コントロール ルールをトラフィックと照合します。ほとんどの場合、システムは、*すべて*のルールの条件がトラフィックに一致する場合、*最初*のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。アクセス コントロール ルールの *アクション*によって、システムが一致するトラフィックをどのように処理するかが決まります。一致するトラフィックをモニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。ルール アクションを使用したトラフィックの処理とインスペクションの決定（14-8 ページ）を参照してください。

次の図は、4 つの異なるタイプのアクセス コントロール ルールとデフォルト アクションを含むアクセス コントロール ポリシーによって制御されている、インラインの侵入防御と AMP の展開におけるトラフィックのフローを示します。



上記のシナリオでは、ポリシー内の最初の 3 つのアクセス コントロール ルール（モニタ、信頼およびブロック）は一致するトラフィックを検査できません。モニタ ルールはネットワーク トラフィックの追跡とロギングを行いますが検査はしないので、システムは引き続きトラフィックを追加のルールと照合し、許可または拒否を決定します。信頼ルールおよびブロック ルールは、どのような種類のインスペクションも追加で行うことなく一致するトラフィックを処理しますが、一致しないトラフィックは引き続き次のアクセス コントロール ルールに照合されます。

ポリシー内の 4 番目と最後のルールである許可ルールは、次の順序で他のさまざまなポリシーを呼び出し、一致するトラフィックを検査および処理します。

- **検出:ネットワーク検出ポリシー:**最初に、ネットワーク検出ポリシーは検出データについてトラフィックを検査します。検出はパッシブ分析で、トラフィックのフローに影響しません。検出は明示的には有効にしませんが、拡張したり無効にしたりすることができます。ただし、トラフィックを許可することで、検出データの収集が自動的に保証されるものではありません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、検出を実行します。詳細については、ネットワーク検出の概要（45-1 ページ）を参照してください。
- **高度なマルウェア防御およびファイル制御:ファイル ポリシー:**トラフィックが検出によって検査された後、システムは禁止されたファイルやマルウェアについてトラフィックを検査できます。ネットワークベースの AMP は、PDF、Microsoft Office 文書など多数のファイル タイプに潜むマルウェアを検出し、オプションでブロックできます。組織がマルウェア ファイル伝送のブロックに加えて、（ファイルにマルウェアが含まれるかどうかに関係なく）特定のタイプのすべてのファイルをブロックする必要がある場合は、*ファイル制御*機能により、特定のファイル タイプの伝送についてネットワーク トラフィックをモニタし、ファイルをブロックまたは許可することができます。
- **侵入防御:侵入ポリシー:**ファイル インスペクションの後、システムは侵入およびエクスプロイトについてトラフィックを検査できます。侵入ポリシーは、デコードされたパケットの攻撃をパターンに基づいて調査し、悪意のあるトラフィックをブロックしたり、変更したりできます。侵入ポリシーは*変数セット*とペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映することができます。
- **宛先:**前述のすべてのチェックを通過したトラフィックは、その宛先に渡されます。

インタラクティブ ブロック ルール（この図には表示されていません）には、許可ルールと同じインスペクション オプションがあることに留意してください。これにより、あるユーザが警告ページをクリック スルーすることによってブロックされた Web サイトをバイパスした場合に、悪意のあるコンテンツがないかトラフィックを検査できます。詳細については、インタラクティブ ブロッキング アクション:ユーザが Web サイト ブロックをバイパスすることを許可する（14-11 ページ）を参照してください。

ポリシー内のモニタ以外のアクセス コントロール ルールのいずれにも一致しないトラフィックは、デフォルト アクションによって処理されます。このシナリオでは、デフォルト アクションは侵入防御アクションとなり、トラフィックは指定された侵入ポリシーを通過する限りその最終宛先に許可されます。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルト アクションが存在する場合があります。表 12-4（12-8 ページ）を参照してください。システムはデフォルト アクションによって許可されたトラフィックに対し検出データおよび侵入の有無を検査できますが、禁止されたファイルまたはマルウェアの有無は検査できないことに注意してください。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

（注） 場合によっては、接続がアクセス コントロール ポリシーによって分析される場合、システムはトラフィックを処理するアクセス コントロール ルール（存在する場合）を決定する前に、その接続の最初の数パケットを処理し**通過を許可する**必要があります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。詳細については、アクセス コントロールのデフォルト侵入ポリシーの設定（25-1 ページ）を参照してください。

上記のシナリオの詳細と、ファイル ポリシーおよび侵入ポリシーをアクセス コントロール ルールおよびアクセス コントロールのデフォルト アクションに関連付ける手順については、以下を参照してください。

- ファイル インスペクションおよび侵入インスペクションの順序について（18-5 ページ）
- AMP またはファイル制御を実行するアクセス コントロール ルールの設定（18-7 ページ）
- 侵入防御を実行するアクセス コントロール ルールの設定（18-8 ページ）
- ネットワーク トラフィックに対するデフォルトの処理とインスペクションの設定（12-8 ページ）

ファイル インスペクションおよび侵入インスペクションの順序について

ライセンス：Protection または Malware

サポートされるデバイス：機能に応じて異なる

サポートされる防御センター：機能に応じて異なる

許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション（18-2 ページ）のシナリオでは、ファイル ポリシーと侵入ポリシーの両方に関連付けられている許可ルールを含む、各タイプのアクセス コントロール ルールを 1 つ示しています。アクセス コントロール ポリシーで、複数の許可ルールとインタラクティブ ブロック ルールを異なる侵入ポリシーおよびファイル ポリシーに関連付けて、インスペクション プロファイルをさまざまなタイプのトラフィックに照合できます。

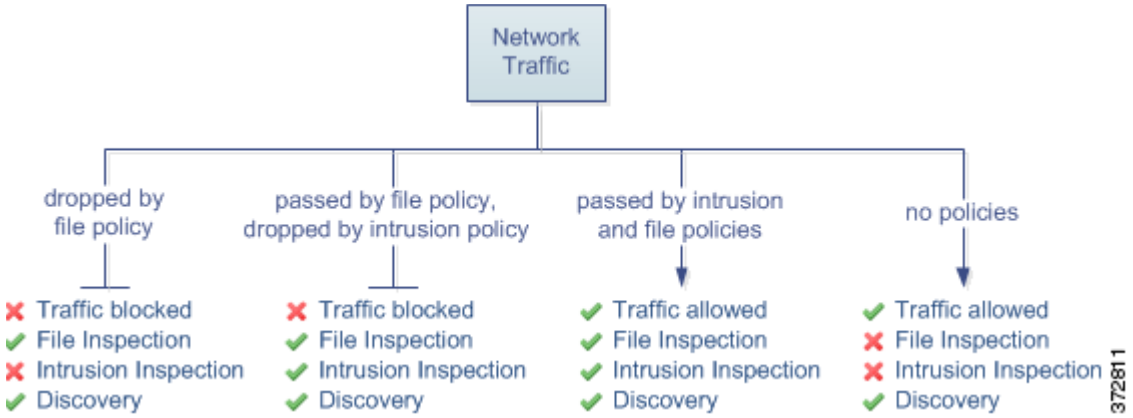
（注） 侵入防御またはネットワーク検出のみのデフォルト アクションによって許可されたトラフィックは、検出データおよび侵入の有無について検査されますが、禁止されたファイルまたはマルウェアの有無については検査されません。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

同じルールでファイル インスペクションと侵入インスペクションの両方を実行する必要はありません。許可ルールまたはインタラクティブ ブロック ルールに一致する接続の場合：

- ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーによって決まります
- 侵入ポリシーがない場合、トラフィック フローはファイル ポリシーによって決まります
- どちらもない場合、許可されたトラフィックはネットワーク検出のみで検査されます

ヒント システムは、信頼されたトラフィックに対してはどんなインスペクションも実行しません。侵入ポリシーもファイル ポリシーも含めずに許可ルールを設定すると、信頼ルールの場合と同様にトラフィックが通過しますが、許可ルールでは一致するトラフィックに対して検出を実行できます。

以下の図は、許可アクセス コントロール ルール、またはユーザによりバイパスされたインタラクティブ ブロック アクセス コントロール ルールのどちらかの条件を満たすトラフィックに対して実行できるインスペクションの種類を示しています。単純化のために、侵入/ファイル ポリシーの両方が 1 つのアクセス コントロール ルールに関連付けられている（またはどちらも関連付けられていない）状態でのトラフィック フローを図に示しています。



アクセス コントロール ルールによって処理される単一接続の場合、ファイル インスペクションは侵入インスペクションの前に行われます。つまり、システムは侵入のためファイル ポリシーによってブロックされたファイルを検査しません。ファイル インスペクション内では、タイプによる単純なブロッキングの方が、マルウェア インスペクションおよびブロッキングよりも優先されます。

たとえば、アクセス コントロール ルールで定義された特定のネットワーク トラフィックを正常に許可するシナリオを考えてください。ただし、予防措置として、実行可能ファイルのダウンロードをブロックし、ダウンロードされた PDF のマルウェア インスペクションを行って検出された場合はブロックし、トラフィックに対して侵入インスペクションを実行する必要があるとします。

一時的に許可するトラフィックの特性に一致するルールを持つアクセス コントロール ポリシーを作成し、それを侵入ポリシーとファイル ポリシーの両方に関連付けます。ファイル ポリシーはすべての実行可能ファイルのダウンロードをブロックし、マルウェアを含む PDF も検査およびブロックします。

- まず、システムはファイル ポリシーで指定された単純なタイプ マッチングに基づいて、すべての実行可能ファイルのダウンロードをブロックします。それらはすぐにブロックされるため、これらのファイルはマルウェア クラウド ルックアップの対象にも侵入インスペクションの対象にもなりません。
- 次に、システムは、ネットワーク上のホストにダウンロードされた PDF に対するマルウェア クラウド ルックアップを実行します。マルウェア ファイルの性質を持つ PDF はすべてブロックされ、侵入インスペクションの対象にはなりません。
- 最後に、システムはアクセス コントロール ルールに関連付けられている侵入ポリシーを使用して、ファイル ポリシーでブロックされなかったファイルを含む残りのトラフィック全体を検査します。

（注） ファイルがセッションで検出されブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

AMP またはファイル制御を実行するアクセス コントロール ルールの設定

ライセンス：Protection または Malware

サポートされるデバイス：機能に応じて異なる

サポートされる防御センター：機能に応じて異なる

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールをファイル ポリシーに関連付けることができます。ファイル インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なるファイルおよびマルウェアのインスペクション プロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムはファイル ポリシーの設定に従って禁止されたファイル（マルウェアを含む）を検出すると、イベントを Defense Center データベースに自動的にロギングします。ログ ファイルまたはマルウェア イベントが必要ない場合は、アクセス コントロール ルールごとにこのロギングを無効にできます。アクセス コントロール ルールにファイル ポリシーを関連付けた後、アクセス コントロール ルール エディタの [ロギング（Logging）] タブで [ログファイル（Log Files）] チェックボックスをオフにします。詳細については、許可された接続のファイルおよびマルウェア イベント ロギングの無効化（38-10 ページ）を参照してください。

また、システムは、呼び出し元のアクセス コントロール ルールのロギング設定に関係なく、関連付けられた接続の終了を Defense Center データベースにロギングします。ファイル イベントとマルウェア イベントに関連付けられた接続（自動）（38-4 ページ）を参照してください。

注意　ファイル ポリシーをアクセス コントロール ルールに関連付けるか、[なし（None）] を選択してポリシーの関連付けを後から解除すると、アクセス コントロール ポリシーを適用するときに Snort プロセスが再起動され、一時的にトラフィック インスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

アクセス コントロール ルールにファイル ポリシーを関連付けるには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　アクセス コントロール ルールを使用して AMP またはファイル制御を設定するアクセス コントロール ポリシーの横にある編集アイコン（  ）をクリックします。

手順 3　新しいルールを作成するか、または既存のルールを編集します。アクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

アクセス コントロール ルール エディタが表示されます。

手順 4　ルール アクションが [許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定されていることを確認します。

手順 5　[インスペクション（Inspection）] タブを選択します。

[インスペクション（Inspection）] タブが表示されます。

手順 6　アクセス コントロール ルールに一致するトラフィックを検査する場合は [ファイル ポリシー（File Policy）] を選択し、または一致するトラフィックに対するファイル インスペクションを無効にする場合は [なし（None）] を選択します。

表示される編集アイコン（）をクリックし、新しいブラウザ タブでポリシーを編集できます。ファイル ポリシーの作成（37-19 ページ）を参照してください。

手順 7　[追加（Add）] をクリックしてルールを保存します。

ルールが保存されます。変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

侵入防御を実行するアクセス コントロール ルールの設定

ライセンス：Protection

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールを侵入ポリシーに関連付けることができます。侵入インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なる侵入インスペクション プロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する*変数セット*使用します。セット内の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

ヒント　システムによって提供される侵入ポリシーを使用する場合であっても、シスコは、正確にネットワーク環境を反映するためにシステムの侵入変数を設定することを**強く**推奨します。少なくとも、デフォルトのセットにあるデフォルトの変数を変更します。定義済みのデフォルトの変数の最適化（3-20 ページ）を参照してください。

1 つのアクセス コントロール ポリシーで使用可能な一意の侵入ポリシーの数は、ターゲット デバイスのモデルによって異なります。より強力なデバイスは、より多数のポリシーを処理できます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。異なる侵入ポリシー変数セットのペアを各許可ルールおよびインタラクティブ ブロック ルール（およびデフォルト アクション）と関連付けることができますが、ターゲット デバイスが設定されたとおりにインスペクションを実行するのに必要なリソースが不足している場合は、アクセス コントロール ポリシーを適用できません。詳細については、パフォーマンスを向上させるためのルールの簡素化（12-26 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侵入ポリシーとカスタム侵入ポリシーについて

シスコは、複数の侵入ポリシーを FireSIGHT システムとともに提供します。システムによって提供される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、詳細設定の初期設定も提供します。システムによって提供されるポリシーをそのまま使用するか、またはカスタム ポリシーのベースとして使用できます。カスタム ポリシーを作成すれば、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。

お客様が独自に作成するカスタム ポリシーに加えて、システムは初期インライン ポリシーと初期パッシブ ポリシーの 2 つのカスタム ポリシーを提供しています。これらの 2 つの侵入ポリシーは、ベースとして Balanced Security and Connectivity 侵入ポリシーを使用します。両者の唯一の相違点は、[インライン時にドロップ（Drop When Inline）] 設定です。インライン ポリシーではドロップ動作が有効化され、パッシブ ポリシーでは無効化されています。詳細については、システム付属ポリシーとカスタム ポリシーの比較（23-8 ページ）を参照してください。

接続イベントおよび侵入イベントのロギング

アクセス コントロール ルールによって呼び出された侵入ポリシーが侵入を検出して侵入イベントを生成すると、そのポリシーはそのイベントを Defense Center データベースに保存します。また、システムはアクセス コントロール ルールのロギング設定に関係なく、侵入が発生した接続の終了を Defense Center データベースに自動的にロギングします。侵入に関連付けられる接続（自動）（38-4 ページ）を参照してください。

注意　侵入ポリシーをアクセス コントロール ルールに関連付けるか、[なし（None）] を選択してポリシーの関連付けを後から解除すると、アクセス コントロール ポリシーを適用するときに Snort プロセスが再起動され、一時的にトラフィック インスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

アクセス コントロール ルールに侵入ポリシーを関連付けるには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　アクセス コントロール ルールを使用して侵入インスペクションを設定するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

手順 3　新しいルールを作成するか、または既存のルールを編集します。アクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

アクセス コントロール ルール エディタが表示されます。

手順 4　ルール アクションが [許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定されていることを確認します。

手順 5　[インスペクション（Inspection）] タブを選択します。

[インスペクション（Inspection）] タブが表示されます。

手順 6　システムによって提供されるまたはカスタムの**侵入ポリシー**を選択するか、またはアクセス コントロール ルールに一致するトラフィックに対する侵入インスペクションを無効にするには [なし（None）] を選択します。

カスタム侵入ポリシーを選択する場合は、表示される編集アイコン（）をクリックし、新しいブラウザ タブでポリシーを編集できます。侵入ポリシーの編集（31-4 ページ）を参照してください。

手順 7　オプションで、侵入ポリシーに関連付けられている**変数セット**を変更します。

表示される編集アイコン（）をクリックし、新しいブラウザ タブで変数セットを編集できます。変数セットの使用（3-19 ページ）を参照してください。

手順 8　[保存（Save）] をクリックしてルールを保存します。

ルールが保存されます。変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

侵入防御パフォーマンスの調整

ライセンス：Protection

シスコは、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を提供しています。これらのパフォーマンス設定は、各アクセス コントロール ポリシーごとに設定し、その設定はその親のアクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシーに適用されます。

詳細については、以下を参照してください。

- 侵入に対するパターン一致の制限（18-10 ページ）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。
- 侵入ルールの正規表現制限のオーバーライド（18-11 ページ）では、Perl 適合正規表現（PCRE）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。
- パケットごとに生成される侵入イベントの制限（18-13 ページ）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。
- パケットおよび侵入ルール遅延しきい値の設定（18-14 ページ） では、パケットとルールの遅延しきい値の設定について説明します。
- 侵入パフォーマンス統計情報のロギングの設定（18-20 ページ）では、管理対象デバイスの基本的なパフォーマンスのモニタリングおよびレポート パラメータを設定する方法について説明します。

侵入に対するパターン一致の制限

ライセンス：Protection

イベント キューで許可するパケット数を指定できます。ストリーム再構成の前後に、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できます。

イベント キューの設定：

アクセス：Admin/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

手順 4　[パフォーマンス設定（Performance Settings）] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [パターン一致の制限（Pattern Matching Limits）] タブを選択します。

手順 5　次のオプションを修正できます。

- [パケットごとに分析するパターン状態の最大値（Maximum Pattern States to Analyze Per Packet）] フィールドに、キューに含めるイベントの最大値の値を入力します。
- ストリーム再構成の前後で、データのより大きなストリームに再構築されるパケットを検査するには、[今後の再構成の対象となるトラフィックでコンテンツ チェックを無効にする（Disable Content Checks on Traffic Subject to Future Reassembly）] 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、データの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無効にするには、[今後の再構成の対象となるトラフィックでコンテンツ チェックを無効にする（Disable Content Checks on Traffic Subject to Future Reassembly）] をオフにします。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。

手順 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

侵入ルールの正規表現制限のオーバーライド

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 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` キーワードの使用については、PCRE を使用したコンテンツの検索（36-39 ページ）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。

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 18-2　正規表現の制約オプション

オプション	説明
検索結果の制限状態（Match Limit State）	[制限に合わせる（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。 • [デフォルト（Default）] を選択して、[制限に合わせる（Match Limit）] に設定した値を使用する • [無制限（Unlimited）] を選択して、無制限の数の試行を許可する • [カスタム（Custom）] を選択して、[制限に合わせる（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
制限に合わせる（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。
検索結果の再起制限状態（Match Recursion Limit State）	[再起制限に合わせる（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。 • [デフォルト（Default）] を選択して、[再起制限に合わせる（Match Recursion Limit）] に設定した値を使用する • [無制限（Unlimited）] を選択して、無制限の数の再帰を許可する • [カスタム（Custom）] を選択して、[再起制限に合わせる（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 [再起制限に合わせる（Match Recursion Limit）] が意味を持つためには、[制限に合わせる（Match Limit）] よりも小さい必要があることに注意してください。
再起制限に合わせる（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/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（ ）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

手順 4　[パフォーマンス設定（Performance Settings）] の横にある編集アイコン（ ）をクリックし、表示されるポップアップ ウィンドウで [正規表現制限（Regular Expression Limits）] タブを選択します。

手順 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。

手順 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

パケットごとに生成される侵入イベントの制限

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 18-3　侵入イベント ロギング制限のオプション

オプション	説明
パケットごとに保存されるイベントの最大数（Maximum Events Stored Per Packet）	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。
パケットごとにログに記録されるイベントの最大数（Maximum Events Logged Per Packet）	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、[パケットごとに保存されるイベントの最大数（Maximum Events Stored Per Packet）] 値を超えてはいけません。
イベント ロギングの順位決定の基準（Prioritize Event Logging 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/Access Admin/Network Admin

手順 1　[ポリシー(Policies)] > [アクセス制御(Access Control)] を選択します。

[アクセス コントロール ポリシー(Access Control Policy)] ページが表示されます。

手順 2　編集するアクセス コントロール ポリシーの横にある編集アイコン( )をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[詳細設定(Advanced)] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

手順 4　[パフォーマンス設定(Performance Settings)] の横にある編集アイコン( )をクリックし、表示されるポップアップ ウィンドウで [侵入イベント ロギング制限(Intrusion Event Logging Limits)] タブを選択します。

手順 5　侵入イベント ロギング制限のオプションの表の任意のオプションを変更できます。

手順 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用(12-17 ページ)を参照してください。

パケットおよび侵入ルール遅延しきい値の設定

ライセンス: Protection

パケットとルールの遅延しきい値の設定では、デバイス遅延を維持します。詳細については、以下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(18-14 ページ)
- パケット遅延しきい値構成の設定(18-16 ページ)
- パケット遅延しきい値構成を無効にするには、次の手順を実行します。(18-17 ページ)
- ルール遅延しきい値構成の設定(18-19 ページ)

パケット遅延しきい値構成について

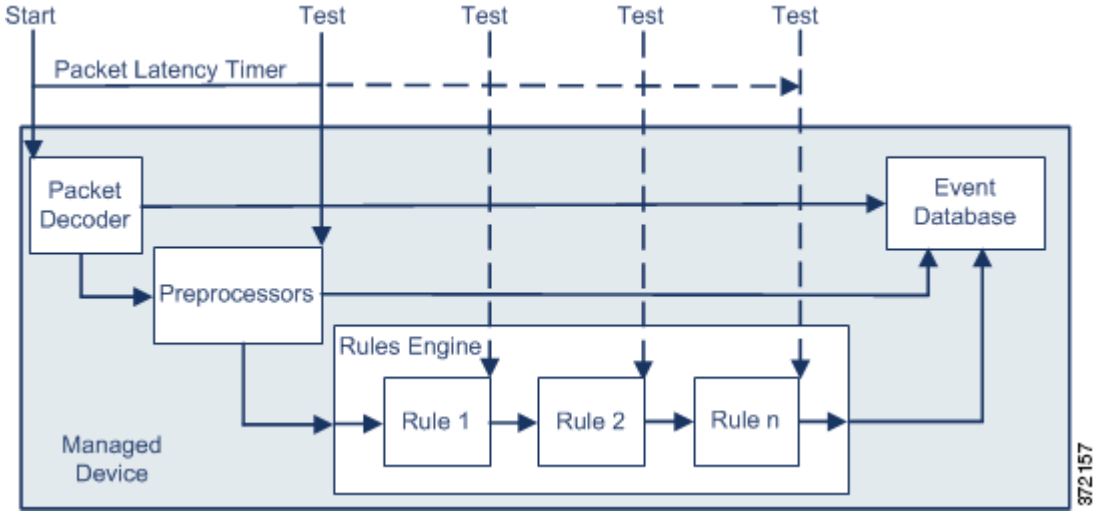
ライセンス: Protection

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。

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

処理時間が任意のテスト ポイントでしきい値を超えると、パケットの検査は停止します。

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（32-23 ページ）を参照してください。

パケット遅延のしきい値は、パッシブおよびインライン展開の両方でシステムのパフォーマンスを向上させ、インライン展開では過度の処理時間を必要とするパケットの検査を停止することにより遅延を低減できます。これらのパフォーマンス上のメリットは、以下のような場合にもたらされます。

- 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。

パケット遅延しきい値構成の設定

ライセンス：Protection

遅延ベースのパフォーマンス設定は、システムによって提供される Balanced Security and Connectivity 侵入ポリシーによってデフォルトで有効になっています。次の表では、パケット遅延しきい値を設定するための単一のオプションについて説明します。

表 18-4　パケット遅延しきい値構成オプション

オプション	説明
しきい値（マイクロ秒）（Threshold (microseconds)）	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。

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、ルール状態の設定（32-23 ページ）を参照してください。

パケット遅延しきい値の設定：

アクセス：Admin/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

手順 4　[遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [パケット処理（Packet Handling）] タブを選択します。

ヒント　デフォルトでは、パケット遅延しきい値構成が有効になっています。遅延しきい値構成を完全に無効にするには、[有効化（Enable）] チェックボックスをオフにします。

手順 5　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

パケット遅延しきい値構成を無効にするには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

手順 4　[遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [パケット処理（Packet Handling）] タブを選択します。

手順 5　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）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は、各ルールが個別のパケットの処理に費やした時間を測定し、処理時間が遅延しきい値ルールをある回数（設定可能）連続して超えた場合は、そのルールに違反した処理を、関連するルールのグループとともに指定された期間中断し、中断期間終了後にルールを回復します。

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。

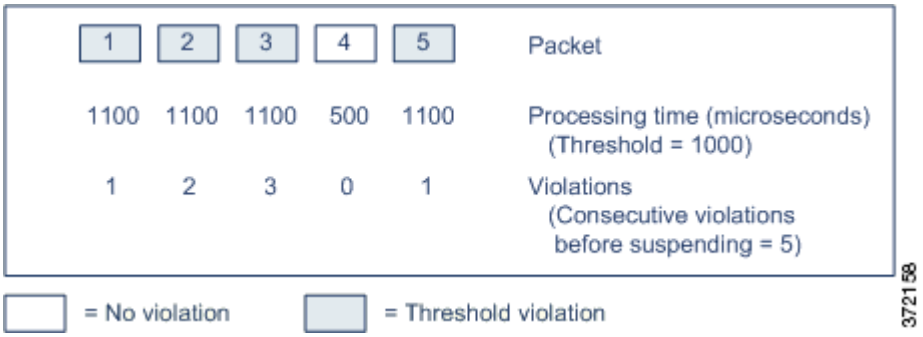
遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。

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

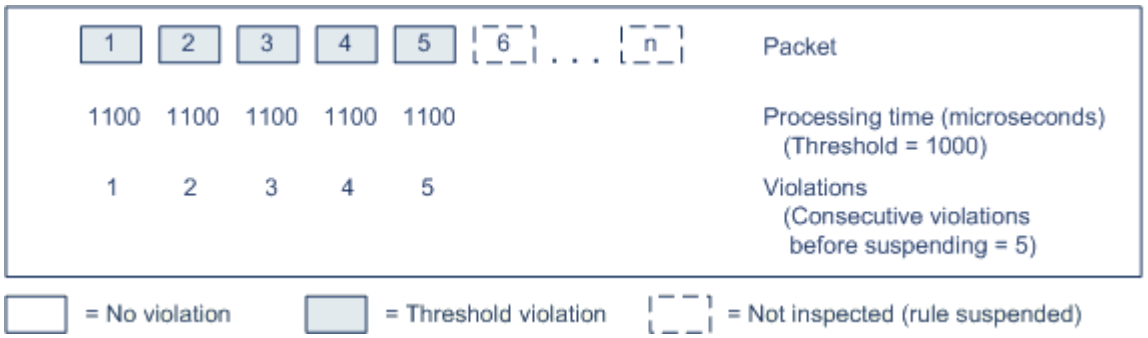
ルールのグループが一時停止しているか、またはルール違反が連続していない場合は、カウンタがゼロになります。ルールを一時停止する前に連続する違反の一部を許可することにより、パフォーマンスへの影響がわずかであると考えられる散発的なルール違反を無視し、繰り返しルール遅延しきい値を超えるルールのより重大な影響に焦点を当てることができます。

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（32-23 ページ）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上のメリットは、以下のような場合にもたらされます。

- 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

ルール遅延しきい値構成の設定

ライセンス：Protection

ルールによるパケット処理時間が、[ルール停止前の連続しきい値違反（Consecutive Threshold Violations Before Suspending Rule）] で指定された回数連続して [しきい値（Threshold）] を超えると、ルール遅延しきい値構成は [停止時間（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（41-10 ページ）とルール状態の設定（32-23 ページ）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 18-5　ルール遅延しきい値構成オプション

オプション	説明
しきい値（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。
ルール停止前の連続しきい値違反（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 [しきい値（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。
停止時間（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。

ルール遅延しきい値の設定：

アクセス：Admin/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

手順 4　[遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある編集アイコン（  ）をクリックし、表示されるポップアップ ウィンドウで [ルール処理（Rule Handling）] タブを選択します。

手順 5　ルール遅延しきい値構成オプションの表の任意のオプションを設定できます。

手順 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

侵入パフォーマンス統計情報のロギングの設定

ライセンス：Protection

デバイスがそのパフォーマンスをモニタおよび報告する動作に関する基本的なパラメータを設定できます。次のオプション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。

[サンプル時間（秒）（Sample time (seconds)）] と [パケットの最小数（Minimum number of packets）]

パフォーマンス統計情報の各更新の間で指定した秒数が経過すると、システムは指定したパケット数を分析したかを検証します。分析していた場合、システムはパフォーマンス統計情報を更新します。それ以外の場合、システムは指定したパケット数を分析するまで待機します。

トラブルシューティング オプション：[ログ セッション/プロトコル分布（Log Session/Protocol Distribution）]

トラブルシューティングの電話中に、プロトコル分布、パケット長、およびポートの統計情報のログを取るようにサポートから依頼される場合があります。

注意　このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

トラブルシューティング オプション：[概要（Summary）]

トラブルシューティングの電話中に、Snort® プロセスのシャット ダウンまたは再起動時に限り、パフォーマンス統計情報を計算するようにシステムを設定するようにサポートから依頼される場合があります。このオプションを有効にするには、[ログ セッション/プロトコル分布（Log Session/Protocol Distribution）] トラブルシューティング オプションも有効にする必要があります。

注意　このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

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/Access Admin/Network Admin

手順 1　[ポリシー(Policies)] > [アクセス制御(Access Control)] を選択します。

[アクセス コントロール ポリシー(Access Control Policy)] ページが表示されます。

手順 2　編集するアクセス コントロール ポリシーの横にある編集アイコン( )をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[詳細設定(Advanced)] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

手順 4　[パフォーマンス設定(Performance Settings)] の横にある編集アイコン( )をクリックし、表示されるポップアップ ウィンドウで [パフォーマンス統計情報(Performance Statistics)] タブを選択します。

手順 5　前述のように、[サンプル時間(Sample time)] または [パケットの最小数(Minimum number of packets)] を変更します。

手順 6　任意で、サポートによって求められた場合にのみ、[トラブルシューティング オプション(Troubleshoot Options)] セクションを展開し、そのオプションを変更します。

手順 7　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用(12-17 ページ)を参照してください。

ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整

ライセンス: Protection または Malware

サポートされるデバイス: 機能に応じて異なる

サポートされる防御センター: 機能に応じて異なる

ファイル制御、ファイル ストレージ、動的分析、あるいはマルウェアの検出またはブロッキングを行うためにファイル ポリシーを使用する場合は、次の表にリストするオプションを設定できます。ファイル サイズを増やすと、システムのパフォーマンスに影響を与える可能性があることに注意してください。

注意　アクセス コントロール ポリシーの値を変更すると、[ファイルおよびマルウェアの設定(Files and Malware Settings)] の詳細設定により、アクセス コントロール ポリシーを適用するときに Snort プロセスが再起動され、一時的にトラフィック インスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort の再開によるトラフィックへの影響(1-9 ページ)を参照してください。

表 18-6　アクセス コントロール ファイルおよびマルウェア検出の詳細オプション

フィールド	説明	デフォルト値（Default Value）	範囲	注記（Notes）
ファイルタイプを検知する前に検閲するバイト数制限（Limit the number of bytes inspected when doing file type detection）	ファイル タイプを検出するときに検査するバイト数を指定します。	1460 バイト、または TCP パケットの最大セグメント サイズ	0 ～ 4294967295（4GB）	制限を取り除くには、0 に設定します。 ほとんどの場合、システムは最初のパケットによって、一般的なファイル タイプを特定できます。
SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）	システムが特定のサイズを超えるファイルを保管すること、ファイルで Collective Security Intelligence クラウド ルックアップを実行すること、またはカスタム検出リストに追加されたファイルをブロックすることを防止します。	10485760（10MB）	0 ～ 4294967295（4GB）	制限を取り除くには、0 に設定します。 この値は、[保存する最大ファイルサイズ（バイト）（Maximum file size to store (bytes)）] および [動的分析テストの最大ファイルサイズ（バイト）（Maximum file size for dynamic analysis testing (bytes)）] の値以上に設定する必要があります。
ファイルを許可するのにかかるマルウェア ブロックのクラウド ルックアップの制限時間（秒）（Allow file if cloud lookup for Block Malware takes longer than (seconds)）	マルウェア クラウド ルックアップの実行中に、システムが [マルウェア ブロック（Block Malware）] ルールに一致し、性質がキャッシュに入れられていないファイルを保持する期間を指定します。システムが性質を取得する前にこの期間が満了すると、ファイルが渡されます。「使用不可」の性質はキャッシュに入れられません。	2 秒	0 ～ 30 秒	このオプションは最大 30 秒に設定できますが、シスコではデフォルト値を使用して、接続失敗によってトラフィックがブロックされないようにすることを推奨します。サポートに連絡することなくこのオプションを 0 に設定**しない**でください。
保存する最小ファイル サイズ（バイト）（Minimum file size to store (bytes)）	システムがファイル ルールを使用して保存できるファイルの最小サイズを指定します。	6144（6KB）	0 ～ 10485760（10MB）	ファイル ストレージを無効にするには、0 に設定します。 このフィールドは、[保存する最大ファイル サイズ（バイト）（Maximum file size to store (bytes)）] および [SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。

表 18-6　アクセス コントロール ファイルおよびマルウェア検出の詳細オプション（続き）

フィールド	説明	デフォルト値（Default Value）	範囲	注記（Notes）
保存する最大ファイル サイズ（バイト）（Maximum file size to store (bytes)）	システムがファイル ルールを使用して保存できるファイルの最大サイズを指定します。	1048576（1MB）	0 ～ 10485760（10MB）	ファイル ストレージを無効にするには、0 に設定します。 このフィールドは、[保存する最小ファイル サイズ（バイト）（Minimum file size to store (bytes)）] の値以上、および [SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。
動的分析テストの最小ファイル サイズ（バイト）（Minimum file size for dynamic analysis testing (bytes)）	システムがクラウドに動的分析対象として送信できるファイルの最小サイズを指定します。	6144（6KB）	6144（6KB）～ 2097152（2MB）	このフィールドは、[動的分析テストの最大ファイル サイズ（バイト）] および [SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。 システムはクラウドをチェックして、送信可能なファイルの最小サイズが更新されているかどうかを調べます（最大で 1 日 1 回）。新しい最小サイズが現在の値より大きい場合、現在の値が新しい最小サイズに更新され、ポリシーは古いポリシーとしてマークされます。

表 18-6　アクセス コントロール ファイルおよびマルウェア検出の詳細オプション(続き)

フィールド	説明	デフォルト値（Default Value）	範囲	注記（Notes）
動的分析テストの最大ファイル サイズ（バイト）（Maximum file size for dynamic analysis testing (bytes)）	システムがクラウドに動的分析対象として送信できるファイルの最大サイズを指定します。	1048576（1MB）	6144（6KB）～ 2097152（2MB）	このフィールドは、[動的分析テストの最小ファイル サイズ（バイト）（Minimum file size for dynamic analysis testing (bytes)）] の値以上、[SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。 システムはクラウドをチェックして、送信可能なファイルの最大サイズが更新されているかどうかを調べます（最大で 1 日 1 回）。新しい最大サイズが現在の値より小さい場合、現在の値が新しい最大サイズに更新され、ポリシーは古いポリシーとしてマークされます。

DC500 では Malware ライセンスを使用できず、シリーズ 2 デバイスまたは Blue Coat X-Series 向け Cisco NGIPS で Malware ライセンスを有効にすることもできないことに注意してください。このため、これらのアプライアンスを使用して個別のファイルをキャプチャ、保存、ブロックしたり、アーカイブ ファイルの内容を分析したり、動的分析用にファイルを送信したり、マルウェア クラウド ルックアップの対象となるファイルのファイル トラジェクトリを表示したりすることはできません。

ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージを設定するには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（ ）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

手順 4　[ファイルおよびマルウェアの設定（Files and Malware Settings）] の横にある編集アイコン（ ）をクリックします。

[ファイルおよびマルウェアの設定（Files and Malware Settings）] ポップアップ ウィンドウが表示されます。

手順 5　アクセス コントロール ファイルおよびマルウェア検出の詳細オプションの表の任意のオプションを設定できます。

手順 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。