侵入ポリシーの詳細設定の使用

*詳細設定*とは、設定するのに特定の専門知識を必要とする、プリプロセッサなどの侵入ポリシー検出やパフォーマンスの設定のことです。通常、詳細設定はほとんど、あるいはまったく変更する必要がありません。詳細設定は導入環境ごとに異なります。

詳細設定は有効/無効にしたり、変更したりできます。デフォルトで有効になる詳細設定や、詳細設定ごとのデフォルトは、侵入ポリシーの基本ポリシーに応じて決まります。詳細については、「基本ポリシーについて」（P.20-17）を参照してください。

特定の標準テキスト ルール、共有オブジェクト ルール、およびプリプロセッサ ルールが正しく動作するためには、一部の詳細設定を有効にする必要があります。必須の詳細設定が無効になっている侵入ポリシーを保存しようとすると、その必須の詳細設定をシステムが自動的に有効にするかどうか尋ねられます。

Web インターフェイスでは、一部の拡張設定オプションがトラブルシューティング オプションとして識別されます。これらのオプションを使用する際には、必ずサポートの支援を受ける必要があります。

詳細については、次の項を参照してください。

- 「詳細設定の変更」（P.22-2）。詳細設定の設定ページにアクセスする方法について説明し、侵入ポリシー内で有効化、無効化、および設定できる詳細設定をリストします。
- 「プリプロセッサについて」（P.22-5）。ルール エンジンで使用できるように、プリプロセッサでトラフィックを正規化する方法を示します。
- 「詳細設定の自動有効化」（P.22-12）。プリプロセッサなどの、有効なルールやルール オプションで必要な詳細設定を自動的に有効にする方法について説明します。
- 「トラブルシューティング オプションについて」（P.22-14）。サポートから指示された場合だけ設定する必要があるトラブルシューティング オプションについて説明します。
- 「侵入ポリシーでのレイヤの使用」（P.23-1）。ルール属性と詳細設定の個別の設定で構成された侵入ポリシー層を追加して、複雑なネットワーク内で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説明します。

詳細設定の変更

ライセンス：Protection

ナビゲーション パネルで [Advanced Settings] を選択すると、[Advanced Settings] ページが表示され、詳細設定がタイプ別にリストされます。このページで、侵入ポリシー内の詳細設定を有効または無効にしたり、詳細設定の設定ページにアクセスしたりできます。

詳細設定を行うには、それを有効にする必要があります。詳細設定を行ってから無効にすると、その設定は保持されます。詳細設定を有効にすると、その詳細設定に関する設定ページへのサブリンクがナビゲーション パネル内の [Advanced Settings] リンクの下に表示され、この設定ページへの [Edit] リンクが [Advanced Settings] ページ上の詳細設定の横に表示されます。詳細設定を無効にすると、詳細設定のサブリンクと [Edit] リンクは表示されなくなります。

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えるようにするためのものです。

詳細設定を変更する場合、変更する設定と、その変更がネットワークに及ぼす可能性のある影響について理解していることが必要です。次の項では、詳細設定ごとに固有の設定の詳細情報へのリンクを記述します。

アプリケーション層プリプロセッサ

アプリケーション層プロトコル デコーダは、特定のタイプのパケット データを、ルール エンジンで分析できる形式に正規化します。詳細については、次の表を参照してください。

表 22-1　アプリケーション層プリプロセッサの設定

設定	参照先
DCE/RPC の設定	「DCE/RPC プリプロセッサの設定」（P.25-13）
DNS の設定	「DNS プリプロセッサの設定」（P.25-19）
FTP および Telnet の設定	「FTP および Telnet トラフィックのデコード」（P.25-21）
HTTP の設定	「HTTP トラフィックのデコード」（P.25-34）
Sun RPC の設定	「Sun RPC プリプロセッサの設定」（P.25-50）
SIP の設定	「SIP プリプロセッサの設定」（P.25-54）
GTP コマンド チャネルの設定	「GTP コマンド チャネルの設定」（P.25-56）
IMAP の設定	「IMAP プリプロセッサの設定」（P.25-59）
POP の設定	「POP プリプロセッサの設定」（P.25-63）
SMTP の設定	「SMTP デコードの設定」（P.25-70）
SSH の設定	「SSH プリプロセッサ オプションの選択」（P.25-74）
SSL の設定	「SSL プリプロセッサの設定」（P.25-80）

SCADA プリプロセッサ

Modbus と DNP3 のプリプロセッサは、トラフィックの異常を検出し、インスペクションのためにデータをルール エンジンに提供します。

表 22-2　SCADA プリプロセッサの設定

設定	参照先
Modbus の設定	「Modbus プリプロセッサの設定」（P.25-81）
DNP3 の設定	「DNP3 プリプロセッサの設定」（P.25-83）

トランスポート層/ネットワーク層プリプロセッサ

ネットワーク層とトランスポート層のプリプロセッサは、ネットワーク層とトランスポート層でエクスプロイトを検出します。パケットがプリプロセッサに送信される前に、パケット デコーダにより、パケット 見出しとペイロードが、プリプロセッサやルール エンジンで簡単に使用できる形式に変換されます。また、パケット 見出し内でさまざまな異常動作が検出されます。

表 22-3　トランスポート層とネットワーク層のプリプロセッサの設定

設定	参照先
チェックサムの検証	「チェックサムの検証」（P.26-1）
検出の設定	「VLAN 見出しの無視」（P.26-2）
インライン正規化	「インライン トラフィックの正規化」（P.26-4）
IP の最適化	「IP デフラグの設定」（P.26-15）
パケットの復号化	「パケットのデコードの設定」（P.26-20）
TCP ストリームの設定	「TCP ストリームの前処理の設定」（P.26-32）
UDP ストリームの設定	「UDP ストリームの前処理の設定」（P.26-35）

特定の脅威の検出

Back Orifice プリプロセッサは、Back Orifice マジック クッキーについて UDP トラフィックを分析します。スキャン アクティビティを報告するようにポートスキャン ディテクタを設定できます。レートベースの攻撃防御は、ネットワークを圧迫するように設計された SYN フラッドや膨大な同時接続からネットワークを保護するのに役立ちます。機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。

表 22-4　特定の脅威の検出の設定

設定	参照先
Back Orifice の検出	「バック オリフィスの検出」（P.28-1）
ポートスキャンの検出	「ポートスキャン検出の設定」（P.28-6）
レートベースの攻撃防御	「レート ベース攻撃防止の設定」（P.28-19）
機密データの検出	「センシティブ データ検出の設定」（P.28-25）

検出の拡張

適応型プロファイルを使用すると、トラフィックをネットワーク マップのホスト情報と関連付けて、それに応じてトラフィックを処理することにより、システムをネットワーク トラフィックに適応させることができます。

表 22-5　検出の拡張の設定

設定	参照先
適応型プロファイル	「適応型プロファイルの設定」（P.29-3）

侵入ルールのしきい値

グローバル ルールのしきい値を設定すると、しきい値を使用して、システムが侵入イベントを記録したり表示したりする回数を制限できるので、多数のイベントでシステムが圧迫されないようにすることができます。

表 22-6　侵入ルールのしきい値の設定

設定	参照先
グローバル ルールのしきい値	「グローバルしきい値の設定」（P.30-3）

パフォーマンス設定

システムには、システム パフォーマンスを向上させるサーバ設定が設けられています。

表 22-7　パフォーマンス設定

設定	参照先
イベント キューの設定	「イベント キュー設定」（P.24-1）
遅延ベースのパケット処理	「パケットしきい値構成の設定」（P.24-5）
遅延ベースのルール処理	「ルール遅延しきい値構成の設定」（P.24-9）
パフォーマンス統計情報の設定	「パフォーマンス統計情報の設定」（P.24-10）
正規表現の制限	「正規表現の制約」（P.24-11）
ルール処理の設定	「ルール処理の設定」（P.24-13）

外部応答

Web インターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、syslog ファシリティへのロギングを有効にしたり、イベント データを SNMP トラップ サーバに送信したりできます。侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。

表 22-8　外部応答の設定

設定	参照先
SNMP アラート	「SNMP 応答の設定」（P.31-3）
syslog アラート	「syslog 応答の設定」（P.31-6）

詳細設定を変更するには、以下を行います。

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。

別のポリシーでまだ保存されていない変更がある場合、それらの変更を破棄して続行するには [OK] をクリックします。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　変更する詳細設定を選択するには、左側のナビゲーション パネルで [Advanced Settings] をクリックし、設定が無効になっている場合は有効にして、[Edit] をクリックします。

設定ページが表示されます。選択した詳細設定の設定オプションをどれでも変更できます。

有効になっている詳細設定の設定ページにアクセスするには、左側のナビゲーション パネルの [Advanced Settings] を展開してから、詳細設定の名前をクリックすることもできます。

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えるようにするためのものです。

ステップ 4　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状態での終了を行います。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。

プリプロセッサについて

ライセンス：Protection

プリプロセッサは、トラフィックを再フォーマットして、ホストで受信されるトラフィックとルール エンジンで読み取られるトラフィックが同じ形式になるようにします。前処理を実行しないと、プロトコルが違うためにパターン マッチングを行えなくなるので、システムでトラフィックを適切に評価できません。シスコのプリプロセッサは、トラフィックを標準化し、ネットワーク層やトランスポート層のプロトコルの異常を識別するのに役立ちます。そのために、不適切な見出し オプションの識別、IP データグラムの最適化、TCP のステートフル インスペクションとストリーム再構成の提供、UDP ストリームの前処理の提供、アプリケーション プロトコルのコマンド構文の解決、チェックサムの検証を行います。

システムで分析されるパケットが、ネットワーク上のホストで処理されるパケットにできるだけ近いものになるように、これらのプリプロセッサを設定できます。各プリプロセッサにはさまざまなオプションと設定があり、ご使用のネットワーク環境の必要に合うように設定できます。ご使用のネットワーク トラフィックにとって適切なプリプロセッサだけを実行して、誤検出や検出漏れを最小限にし、パフォーマンスを最適化できます。

一般に、侵入検知および防御システムがネットワークを保護する上で重要なコンポーネントになるほど、このシステム自体が攻撃者のターゲットになります。たとえば攻撃者は、意図的に DoS 攻撃を作成するために、スプーフィングされた送信元 IP アドレスの SYN パケットを送信して、受信側のサーバーが保留中の TCP 接続用にメモリを割り当てるようにすることがあります。その後、サーバは SYN-ACK を発信 IP アドレスに送信し、TCP セッションを確立します。

攻撃者が正当な IP アドレスを使用していないので、SYN-ACK メッセージはタイムアウトになり、サーバはメッセージを再送するので、長期間メモリが割り当てられたままになります。このようなハーフオープン TCP 接続はシステム リソースを消耗させます。ほとんどのシステムは TCP セッションに対してステートフル インスペクションを実行しようとするので、システムはこの種のオープン TCP セッションの状態を確立しようとしている間に DoS 状態になる可能性があります。しかし、システムの一部として組み込まれているトランスポート層プリプロセッサは、TCP 接続の状態を検出し、ハーフオープン接続をなくして、誤接続によるルール エンジンの過負荷を防止できます。

プリプロセッサ オプションは、管理対象デバイス自体に対する攻撃から保護するので、ネットワークの高可用性とセキュリティ向上が保障されます。多くのプリプロセッサ オプションは、トリガー時にイベントを生成できるプリプロセッサ ルールと関連付けられます。インラインで FireSIGHT システムを展開している場合、インライン侵入ポリシー内のプリプロセッサ ルールの状態を、悪意のあるパケットをドロップするように設定できます。イベントを生成するようにルールを設定することの詳細と、インライン展開でパケットをドロップすることの詳細については、「ルール状態の設定」（P.21-22）を参照してください。

プリプロセッサ ルールに関するルール状態、しきい値、抑制、レートベースのルール状態、アラート、ルール コメントを設定できます。プリプロセッサ ルールは、侵入ポリシーの [Rules] ページ上の [Preprocessors] フィルタ グループ内と、[Category] フィルタ グループ内のプリプロセッサとパケット デコーダのサブグループ内で、プリプロセッサごとにリストされます。プリプロセッサとデコーダのルールの状態を [Generate Events] に設定するか、必要に応じて、インライン展開で [Drop and Generate events] に設定する（プリプロセッサかパケット デコーダに侵入イベントを記録させる場合）必要があります。プリプロセッサ ルールを有効にすると、ポリシーに保存されていない変更が含まれている場合には、ステータス メッセージが [Policy Information] ページの下部に表示されることに注意してください。詳細については、「侵入ポリシーの編集」（P.20-7）、「侵入ポリシー内のルールの管理」（P.21-1）、および「ルール状態の設定」（P.21-22）を参照してください。

システムでは、プリプロセッサに加えて、異常なトラフィックの検出、検出の拡張、グローバル ルールしきい値の適用、パフォーマンスの調整、および外部 SNMP の設定、syslog アラートに関する詳細設定も提供されています。

詳細については、次の項を参照してください。

- 「プリプロセッサ使用時のトラフィックの課題への対応」（P.22-6）。ネットワーク層、トランスポート層、およびアプリケーション層で生じる通常のトラフィックとインスペクションの課題について説明します。
- 「プロセッサの実行順について」（P.22-7）。FireSIGHT システム プリプロセッサの実行順序について説明します。
- 「プロセッサ イベントの読み取り」（P.22-9）。プリプロセッサ イベントと含まれる情報について説明します。

プリプロセッサ使用時のトラフィックの課題への対応

ライセンス：Protection

システムは、モニタ対象のネットワークのセグメントを通過するトラフィックのインスペクションを行います。これは簡単なことに思えますが、データが表される方法が多種多様であり、データが送信される方法に固有の特性があるため、トラフィックのインスペクションは複雑になることがあります。FireSIGHT システムは、通常のトラフィックに固有の課題や、損害を与えたりインスペクションを回避するように設計されているパケットに固有の課題を軽減します。

TCP/IP の各層には、以下の課題があります。

- ネットワーク層とリンク層

  ネットワーク層の通常のトラフィックは断片化されることがあります。つまり、IP データグラムが最大伝送単位を超えると、小さいフラグメントにして伝送する必要があります。攻撃の分析を有効なものにするには、その前に断片化された IP データグラムを再構成する必要があります。また攻撃者が、重複しているフラグメント、複数のゼロオフセット フラグメント（Jolt2 Denial of Service（DoS）攻撃）、断片化されたプロトコル 見出しなどの悪意のある IP フラグメンテーションを使用することがあります。これらはすべて、通常はネットワーク上で許可されないトラフィックをマスクします。さらに、DoS 攻撃を意図した、無効な長さゼロの IP オプションを使用してパケットを細工する攻撃をネットワーク層が受けることがあります。

- トランスポート層

  トランスポート層は TCP ストリームベース攻撃の対象になります。たとえば、シーケンス番号が重複している TCP パケットを送信し、システムにどちらが有効なシーケンス番号か判別するように強制したりします。トランスポート層は TCP 見出し オプション攻撃に対してオープンになっていることがあります。たとえば、TCP パケットをスプーフィングし、見出し値を変更して、TCP 接続を閉塞状態にし、さらに攻撃を伝播したりします。また TCP は状態関連の攻撃の対象となります。たとえば、Stick や Snot によって、確立済みの接続の一部でない TCP パケットが生成され、ルールが大量にトリガーとして使用されて、システムとアナリストに対する DoS 攻撃が行われることがあります。攻撃者は、チェックサムが無効の TCP、UDP、および ICMP パケットを伝送して、宛先ホストで決して受信されないパケットがシステムで検査されるようにする、ごまかし攻撃を加えることもあります。TCP セッションを再構築すると、トラフィックの効率的な分析をサポートするコンテキストがパケットごとに提供されます。

  また、関連付けられている UDP ユーザ データグラムを追跡することにより、攻撃を検出する点でのシステムの特異性を高めることができます。

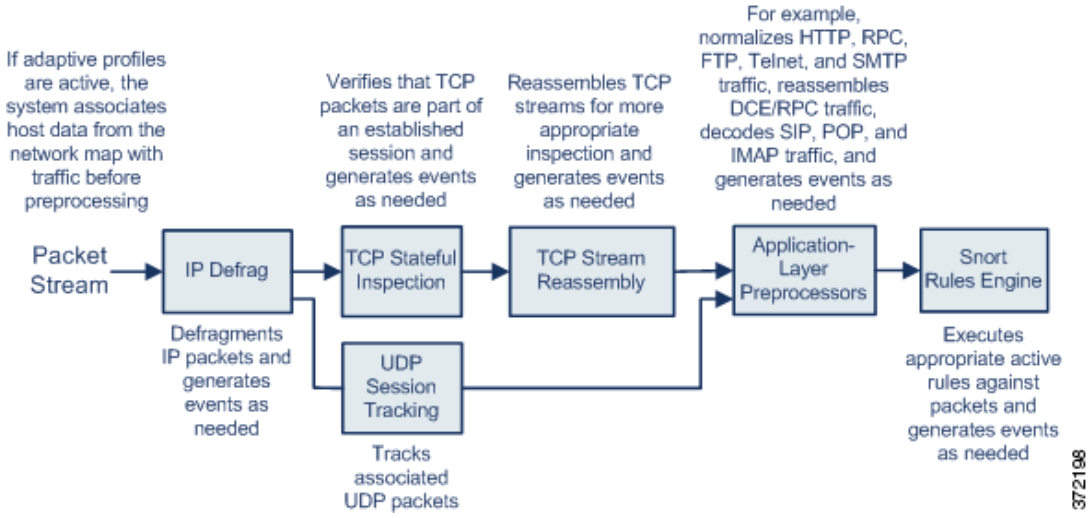
- アプリケーション層

  HTTP、Telnet、FTP、SMTP、RPC などのアプリケーション層プロトコルには、同じデータを表す方法が複数あります。そのため、特定のパケット ペイロードの内容を検査するように設計されたルールが、パケットとルールでペイロードを表す方法が異なるために、失敗することがあります。HTTP、Telnet、FTP、SMTP、RPC パケットを復号化してから、そのデータを標準的な表現に正規化することで、この課題が軽減されます。

プロセッサの実行順について

ライセンス：Protection

プロトコル デコーダ、プリプロセッサ、およびルールは特定の順序で実行され、最初に IP 転送層プロトコルの復号化を実行し、次に必要に応じてデータの正規化を実行してから、その結果のパケットを現在有効なルールに対して評価できるようにします。デフォルト ポリシー設定は、最初に IP 転送層プロトコルの復号化を実行し、次に必要に応じてデータの正規化を実行するようにプリプロセッサを設定します。



このアプローチには次の利点があります。

- システムで、断片化されていて最適化できない IP データグラムに対して侵入イベントを生成してから、これらのパケットの検査を停止できます。
- システムで、状態を検証できない TCP パケットに対してイベントを生成してから、これらのパケットの検査を停止できます。
- システムで、関連 UDP パケットに対してイベントを生成できます。
- 再構成できない TCP パケットや有効な TCP セッションの一部でない TCP パケットが無視されるので、ルールで適切にテストできるパケットだけが正規化され、パフォーマンスが最適化されます。
- システムで、適応型プロファイル、ターゲットベースのポリシー、またはその両方を使用して、IP 最適化およびストリーム前処理の動作をターゲット ホストのオペレーティング システムの形式に合うように調整できます。
- 前処理の後に、ルール エンジンによって、受信ホストでの分析と同じ方法でトラフィックを分析できます。

注意　プリプロセッサは設定に基づいて実行されます。デフォルト設定を変更すると、無効にしたプリプロセッサはシステムによって実行されません。たとえば、トランスポート層プロトコル プリプロセッサを無効にした場合、トランスポート層プロトコル プリプロセッサによって記録され、インスペクションから除外された（パケットのインスペクションが行われた場合）可能性があるパケットに対して、システムはコンテンツ ルールを実行します。これにより、実行順序は変更されないことに注意してください。

プロセッサ イベントの読み取り

ライセンス：Protection

プリプロセッサでは、2 つの機能が提供されています。指定されたアクション（HTTP トラフィックの復号化や正規化など）をパケットに対して実行する機能と、プリプロセッサ オプションおよび関連付けられているプリプロセッサ ルールを有効にしたパケットがトリガーするたびにイベントを生成して、指定されたプリプロセッサ オプションの実行を報告する機能です（たとえば、`Double Encoding` HTTP Inspect オプションと、HTTP Inspect ジェネレータ（GID）が 119 で Snort ID（SID）が 2 の関連付けられているプリプロセッサ ルールを有効にして、プリプロセッサが IIS 二重エンコード トラフィックを検出したときにイベントを生成できます）。プリプロセッサの実行を報告するイベントを生成すると、異常なプロトコル エクスプロイトを検出するのに役立ちます。たとえば、攻撃者は、ホスト上で DoS 攻撃を引き起こす重複 IP フラグメントを細工することがあります。IP 最適化プリプロセッサは、この種の攻撃を検出し、その攻撃に関する侵入イベントを生成できます。

詳細については、次の項を参照してください。

- 「プリプロセッサ イベントのパケットの表示について」（P.22-9）。プリプロセッサで生成されるイベントに含まれる情報について説明します。
- 「プリプロセッサのジェネレータ ID の読み取り」（P.22-9）。プリプロセッサ ジェネレータ ID によって提供される情報について詳しく説明します。

プリプロセッサ イベントのパケットの表示について

ライセンス：Protection

プリプロセッサ イベントは、イベントに関するルールの詳細な説明がパケットの表示に含まれないという点がルール イベントと異なります。代わりに、イベント メッセージ、ジェネレータ ID、Snort ID、パケット 見出し データ、およびパケット ペイロードが、パケットの表示に含まれます。この情報を使用して、パケットの見出し情報を分析し、見出し オプションが使用されているかどうか、およびシステムの脆弱性を攻撃する可能性があるかどうかを判別し、パケット ペイロードを検査できます。プリプロセッサが各パケットを分析した後、ルール エンジンがそのパケットに対して該当するルールを実行して（プリプロセッサがそのパケットを最適化し、有効なセッションの一部として確立できた場合）潜在的なコンテンツ レベルの脅威をさらに分析して報告します。

プリプロセッサのジェネレータ ID の読み取り

ライセンス：Protection

各プリプロセッサには独自のジェネレータ ID 番号、つまり GID があり、これはパケットによってトリガーとして使用されたプリプロセッサを示します。一部のプリプロセッサには関連した SID もあり、これは潜在的な攻撃を分類する ID 番号です。イベントのタイプを分類する方法は、ルールをトリガーするパケットのコンテキストをルールの Snort ID （SID）が提供する方法とほぼ同じなので、イベントを効率的に分析するのに役立ちます。侵入ポリシーの [Rules] ページ上の [Preprocessors] フィルタ グループ内にプリプロセッサ別にプリプロセッサ ルールをリストできます。また、[Category] フィルタ グループ内のプリプロセッサとパケット デコーダのサブグループ内にもプリプロセッサ ルールをリストできます。詳細については、「侵入ポリシー内のルールの管理」（P.21-1）と、「ルール タイプ」表を参照してください。

注　標準テキスト ルールにより生成されるイベントのジェネレータ ID は 1 になります。イベントの SID は、トリガーとして使用された特定のルールを示します。共有オブジェクト ルールの場合、イベントのジェネレータ ID は 3 で、トリガーとして使用された特定のルールを示す SID があります。

次の表では、各 GID を生成するイベントのタイプについて説明しています。

表 22-9　ジェネレータ ID

ID	コンポーネント	説明
1	標準的なテキスト ルール	パケットが標準テキスト ルールをトリガーとして使用したときにイベントが生成されました。詳細については、「ルール タイプ」の表を参照してください。
2	タグ付きパケット	タグ付きセッションからパケットを生成するタグ ジェネレータによって、イベントが生成されました。これは、tag ルール オプションが使用される場合に発生します。詳細については、「攻撃後トラフィックの評価」（P.32-95）を参照してください。
3	共有オブジェクト ルール	パケットが共有オブジェクト ルールをトリガーとして使用したときにイベントが生成されました。詳細については、「ルール タイプ」の表を参照してください。
102	HTTP デコーダ	デコーダ エンジンが、パケット内の HTTP データを復号化しました。
105	Back Orifice ディテクタ	Back Orifice ディテクタが、パケットに関連付けられた Back Orifice 攻撃を特定しました。詳細については、「バック オリフィスの検出」（P.28-1）を参照してください。
106	RPC デコーダ	RPC デコーダがパケットを復号化しました。詳細については、「Sun RPC プリプロセッサの使用」（P.25-49）を参照してください。
116	パケット デコーダ	パケット デコーダによってイベントが生成されました。詳細については、「パケットのデコードについて」（P.26-17）を参照してください。
119、120	HTTP Inspect プリプロセッサ	HTTP Inspect プリプロセッサによってイベントが生成されました。GID 120 ルールがサーバ固有の HTTP トラフィックに関連しています。詳細については、「HTTP トラフィックのデコード」（P.25-34）を参照してください。
122	ポートスキャン ディテクタ	ポートスキャン フロー ディテクタによってイベントが生成されました。詳細については、「ポートスキャンの検出」（P.28-3）を参照してください。
123	IP デフラグメンタ	断片化された IP データグラムを適切に再構成できなかったときに、イベントが生成されました。詳細については、「IP パケットのデフラグ」（P.26-12）を参照してください。
124	SMTP デコーダ	SMTP プリプロセッサが SMTP バーブに対するエクスプロイトを検出したときに、イベントが生成されました。詳細については、「SMTP デコードについて」（P.25-65）を参照してください。
125	FTP デコーダ	FTP/Telnet デコーダが FTP トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。詳細については、「サーバレベルの FTP オプションについて」（P.25-26）および「クライアント レベルの FTP オプションについて」（P.25-31）を参照してください。
126	Telnet デコーダ	FTP/Telnet デコーダが Telnet トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。詳細については、「FTP および Telnet トラフィックのデコード」（P.25-21）を参照してください。

表 22-9　ジェネレータ ID （続き）

ID	コンポーネント	説明
128	SSH プリプロセッサ	SSH プリプロセッサが SSH トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。詳細については、「SSH プロプロセッサによるエクスプロイトの検出」（P.25-73）を参照してください。
129	ストリーム プリプロセッサ	ストリーム プリプロセッサによるストリームの前処理中に、イベントが生成されました。詳細については、「TCP ストリームの前処理の使用」（P.26-21）を参照してください。
131	DNS プリプロセッサ	DNS プリプロセッサによってイベントが生成されました。詳細については、「DNS ネーム サーバ応答におけるエクスプロイトの検出」（P.25-16）を参照してください。
133	DCE/RPC プリプロセッサ	DCE/RPC プリプロセッサによってイベントが生成されました。詳細については、「DCE/RPC トラフィックのデコード」（P.25-2）を参照してください。
134	ルール遅延、パケット遅延	ルール遅延によって侵入ルールのグループが中断された（134:1）または再有効化された（134:2）とき、あるいはパケット遅延しきい値が超過したためにシステムがパケットの検査を停止したとき（134:3）に、イベントが生成されました。詳細については、「パケット遅延しきい値構成について」（P.24-2）、「トラブルシューティング オプションについて」（P.22-14）、「ルール遅延しきい値構成について」（P.24-6）を参照してください。
135	レートベースの攻撃ディテクタ	レートベースの攻撃ディテクタがネットワーク上のホストに対する過度の接続を識別したときに、イベントが生成されました。詳細については、「レートベース攻撃の防止」（P.28-10）を参照してください。
138、139	機密データ プリプロセッサ	機密データ プリプロセッサによってイベントが生成されました。詳細については、「センシティブ データの検出」（P.28-20）を参照してください。
140	SIP プリプロセッサ	SIP プリプロセッサによってイベントが生成されました。詳細については、「Session Initiation Protocol のデコード」（P.25-51）を参照してください。
141	IMAP プリプロセッサ	IMAP プリプロセッサによってイベントが生成されました。詳細については、「IMAP トラフィックのデコード」（P.25-57）を参照してください。
142	POP プリプロセッサ	POP プリプロセッサによってイベントが生成されました。詳細については、「POP トラフィックのデコード」（P.25-61）を参照してください。
143	GTP プリプロセッサ	GTP プリプロセッサによってイベントが生成されました。詳細については、「GTP コマンド チャネルの設定」（P.25-56）を参照してください。
144	Modbus プリプロセッサ	Modbus SCADA プリプロセッサによってイベントが生成されました。詳細については、「Modbus プリプロセッサの設定」（P.25-81）を参照してください。
145	DNP3 プリプロセッサ	DNP3 SCADA プリプロセッサによってイベントが生成されました。詳細については、「DNP3 プリプロセッサの設定」（P.25-83）を参照してください。

詳細設定の自動有効化

ライセンス：Protection

詳細設定が標準テキスト ルール、共有オブジェクト ルール、プリプロセッサ ルール、または別の詳細設定で必要になる場合、システムによって有効にできます。ルール、ルール オプション、または他の詳細設定で必要な詳細設定を無効にして侵入ポリシーを保存すると、必須の詳細設定がシステムにより自動的に有効にされるようにするかどうか尋ねられます。ポリシーを保存するには、その前に必須の詳細設定を手動で有効にするか、システムにより必須の詳細設定を自動的に有効にできるようにするか、または詳細設定が必要なルールか他の詳細設定を無効にする必要があります。

未設定の詳細設定がシステムにより自動的に有効にされる際には、デフォルト設定が使用されることに注意してください。

次の表に、さまざまな詳細設定で必要なルールとルール オプションをリストします。

表 22-10　自動的に有効にされる詳細設定

詳細設定のタイプ	詳細設定	自動有効化プロンプトを表示させるルールとルール オプション
アプリケーション層プリプロセッサ	DCE/RPC の設定	キーワード： • byte_jump（DCE/RPC オプションが有効な場合） • byte_test（DCE/RPC オプションが有効な場合） • byte_extract（DCE/RPC オプションが有効な場合） • dce_iface • dce_opnum • dce_stub_data
アプリケーション層プリプロセッサ	HTTP の設定	キーワード： • content（HTTP コンテンツ オプションが有効な場合） • urilen • http_encode • pcre（P、I、C、K、M、Y、U、S、H、D オプションがルール内で使用されている場合）
アプリケーション層プリプロセッサ	SIP の設定	キーワード： • sip_header • sip_body • sip_method • sip_status_code
アプリケーション層プリプロセッサ	GTP コマンド チャネルの設定	キーワード： • gtp_version • gtp_type • gtp_info

表 22-10　自動的に有効にされる詳細設定 （続き）

詳細設定のタイプ	詳細設定	自動有効化プロンプトを表示させるルールとルール オプション
アプリケーション層プリプロセッサ	SSL Configuration	キーワード： • ssl_state • ssl_version
SCADA プリプロセッサ	Modbus の設定	キーワード： • modbus_data • modbus_func • modbus_unit
SCADA プリプロセッサ	DNP3 の設定	キーワード： • dnp3_data • dnp3_func • dnp3_ind • dnp3_obj
トランスポート層/ネットワーク層プリプロセッサ	TCP または UDP ストリームの設定	キーワード： • flow • flowbits • stream_size
トランスポート層/ネットワーク層プリプロセッサ	TCP ストリームの設定	キーワード：stream_reassemble
特定の脅威の検出	機密データの検出	ジェネレータ ID： • 138 • 139
パフォーマンス設定	正規表現の制限	キーワード：pcre

ストリームの前処理が必要なプリプロセッサを有効にしている場合、ストリームの前処理を無効にしていると、ポリシーを保存する際に、該当するプロトコルに関するストリームの前処理を有効にするかどうか尋ねられます。

TCP ストリームの前処理を有効にするかどうか尋ねられるのは、この処理を無効にしており、以下のプリプロセッサを有効にしている場合です。

- DCE/RPC プリプロセッサ（RPC over HTTP プロキシ、RPC over HTTP サーバ、TCP、または SMB トランスポート プロトコルが選択されている場合）
- DNS プリプロセッサ
- FTP/Telnet プリプロセッサ
- HTTP インスペクト プリプロセッサ
- IMAP プリプロセッサ
- POP プリプロセッサ
- SMTP プリプロセッサ

- SSL プリプロセッサ
- Modbus プリプロセッサ
- DNP3 プリプロセッサ
- ポートスキャン検出（TCP プロトコルが選択されている場合）
- レートベースの攻撃防御
- 機密データの検出

UDP ストリームの前処理を有効にするかどうか尋ねられるのは、この処理を無効にしており、以下のプリプロセッサを有効にしている場合です。

- DCE/RPC プリプロセッサ（UDP トランスポート プロトコルを選択している場合）
- SIP プリプロセッサ
- GTP プリプロセッサ

トラブルシューティング オプションについて

ライセンス：Protection

トラブルシューティングに関する問い合わせの際に、サポートは、1 つ以上のトラブルシューティング オプションを変更するようにお願いすることがあります。トラブルシューティング オプションは、関連する詳細設定の設定ページに表示されます。これらのオプションは詳細設定に関連する他のオプションとともに使用できますが、これらのオプションの設定を変更するとパフォーマンスに影響を及ぼすため、必ずサポートの指示に従って実行する必要があります。

次の表で、これらのトラブルシューティング オプションについて説明します。

表 22-11　トラブルシューティング オプション

詳細設定	オプション	説明
FTP and Telnet Configuration（ポリシー）	Log FTP Command Validation Configuration	この FTP/Telnet のターゲットベースのポリシー オプションを使用することにより、サーバ用にリストされている FTP コマンドごとに設定情報の出力を有効にしたり無効にしたりできます。 詳細については、「サーバレベルの FTP オプションについて」（P.25-26）を参照してください。
Performance Statistics Configuration（グローバル）	Log Session/Protocol Distribution	このグローバル パフォーマンス オプションは、プロトコル分布、パケット長、およびポートの統計情報をログに記録します。 詳細については、「パフォーマンス統計情報の設定」（P.24-10）を参照してください。
Performance Statistics Configuration（グローバル）	Summary	このグローバル パフォーマンス オプションは、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に指示します。 このオプションは、Log Session/Protocol Distribution トラブルシューティング オプションが有効な場合だけ使用できることに注意してください。 詳細については、「パフォーマンス統計情報の設定」（P.24-10）を参照してください。

表 22-11　トラブルシューティング オプション（続き）

詳細設定	オプション	説明
TCP Stream Configuration（グローバル）	Session Termination Logging Threshold	このグローバル TCP オプションは、個々の接続が指定済みのしきい値を超えた場合にメッセージを記録します。 値を 0 にすると、メッセージはオフになります。 上限は 1GB ですが、管理対象デバイス上でストリーム処理のために割り振られるメモリの量によっても制限されます。 詳細については、「TCP ストリームの前処理の使用」（P.26-21）を参照してください。
TCP Stream Configuration（ポリシー）	Maximum Queued Bytes	この TCP のターゲットベースのポリシー オプションは、TCP 接続の片側でキューイングできるデータの量を指定します。 値 0 は、無制限のバイト数を指定します。 詳細については、「TCP ストリームの前処理の使用」（P.26-21）を参照してください。
TCP Stream Configuration（ポリシー）	Maximum Queued Segments	この TCP のターゲットベースのポリシー オプションは、TCP 接続の片側でキューイングできるデータ セグメントの最大バイト数を指定します。 値 0 は、無制限のデータ セグメント バイト数を指定します。 詳細については、「TCP ストリームの前処理の使用」（P.26-21）を参照してください。