CHAPTER 34

特定の脅威の検出

ネットワーク分析ポリシーでさまざまなプリプロセッサを使用して、モニタ対象ネットワークへの特定の攻撃、たとえば、Back Orifice 攻撃、複数のポートスキャン タイプ、過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレート ベース攻撃などを検出できます。ただし、侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーのユーザ インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。詳細については、カスタム ポリシーに関する制約事項（23-13 ページ）を参照してください。

注意 カスタム ユーザ ロールを持つ一部のユーザは、標準メニュー パス（[ポリシー（Policies）] > [アクセス制御（Access Control）] > [ネットワーク分析ポリシー（Network Analysis Policy）]）からネットワーク分析ポリシーにアクセスできません。これらのユーザは、侵入ポリシーを介してネットワーク分析ポリシーにアクセスできます（[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] > [ネットワーク分析ポリシー（Network Analysis Policy）]）。カスタム ユーザ ロールの詳細については、カスタム ユーザ ロールの管理（61-56 ページ）を参照してください。

侵入ポリシーで設定するセンシティブ データ検出を使用して、センシティブな数値データの保護なし送信を検出することもできます。

特定の脅威の検出の詳細については、次の項を参照してください。

- Back Orifice の検出（34-2 ページ）では、Back Orifice 攻撃の検出について説明しています。
- ポートスキャンの検出（34-3 ページ）では、各種のポートスキャンについて概説し、ポートスキャン検出を使用して、攻撃に発展する前にネットワークに対する脅威を識別する方法を説明しています。
- レート ベース攻撃の防止（34-10 ページ）では、サービス妨害（DoS）および SYN フラッド攻撃を制約する方法を説明しています。
- センシティブ データの検出（34-20 ページ）では、ASCII テキストのセンシティブ データ（クレジット カード番号や社会保障番号など）を検出してイベントを生成する方法を説明しています。

Back Orifice の検出

ライセンス：Protection

FireSIGHT システム は、Back Orifice プログラムの存在を検出するプリプロセッサを提供しています。Back Orifice プログラムにより Windows ホストに対する管理者アクセス権を取得される可能性があります。Back Orifice プリプロセッサは、UDP トラフィックを分析し、パケットの最初の 8 バイトにあり XOR で暗号化されている、Back Orifice magic Cookie「`*!*QWTY?`」を調べます。

Back Orifice プリプロセッサには設定ページがありますが、設定オプションはありません。Back Orifice プリプロセッサが有効になっていても、以下の表にリストするプリプロセッサ ルールを有効にしなければ、対応するイベントは生成されません。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。

表 34-1　Back Orifice GID:SID

プリプロセッサ ルール GID:SID	説明
105:1	Back Orifice トラフィック検出
105:2	Back Orifice クライアント トラフィック検出
105:3	Back Orifice サーバ トラフィック検出
105:4	Back Orifice Snort バッファ攻撃検出

[Back Orifice 検知（Back Orifice Detection）] ページを表示する方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス コントロール ポリシー（Access Control Policy）] を選択して [アクセス コントロール ポリシー（Access Control Policy）] ページを表示し、[ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。

[ネットワーク分析ポリシー（Network Analysis 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　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

手順 4　[特定の脅威検知（Specific Threat Detection）] の下の [Back Orifice 検知（Back Orifice Detection）] が有効になっているかどうかによって、2 つの選択肢があります。

- プリプロセッサが有効になっている場合は、[編集（Edit）] をクリックします。
- プリプロセッサが無効になっている場合は、[有効（Enabled）] をクリックしてから、[編集（Edit）] をクリックします。

[Back Orifice 検知（Back Orifice Detection）] 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階層を示します。詳細については、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。

手順 5　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。

ポートスキャンの検出

ライセンス：Protection

ポートスキャンとは、攻撃者が攻撃の準備段階としてよく使用する、ネットワーク調査の形式です。ポートスキャンでは、攻撃者が特別に細工したパケットをターゲット ホストに送信します。攻撃者は多くの場合、ホストが応答するパケットを調べることで、ホストでどのポートが開かれているか、そして開かれているポートでどのアプリケーション プロトコルが実行されているかを、直接あるいは推論によって判断できます。

ポートスキャン検出が有効になっていても、侵入ポリシーの [ルール（Rules）] ページでジェネレータ ID（GID）が 122 に設定されたルールを有効にしなければ、ポートスキャン ディテクタの有効になっているポートスキャン タイプがポートスキャン イベントを生成しないことに注意してください。詳細については、「ルール状態の設定（32-23 ページ）」と「表 34-5（34-8 ページ）」を参照してください。

ポートスキャンは、それ自体では攻撃の証拠になりません。実際、攻撃者が使用するポートスキャン手法の中には、正当なユーザがネットワークで使用する可能性があるものもあります。Cisco のポートスキャン ディテクタは、アクティビティのパターンを検出するという方法で、悪意のあるポートスキャンの可能性があるものを判別できるように設計されています。

攻撃者がネットワークを調査するために複数の手法を使用することはよくあります。通常、攻撃者は異なる複数のプロトコルを使用して、ターゲット ホストからさまざまな応答を引き出します。その目的は、ブロックされた特定タイプのプロトコルを基に、使用できる可能性のあるプロトコルを絞り込んでいくことです。以下の表に、ポートスキャン ディテクタでアクティブにできるプロトコルを記載します。

表 34-2　プロトコル タイプ

プロトコル	説明
TCP	TCP プローブを検出します。たとえば、SYN スキャン、ACK スキャン、TCP connect() スキャン、および Xmas tree、FIN、NULL といった異常なフラグを組み合わせたスキャンなどです。
UDP	UDP プローブを検出します。たとえば、ゼロ バイトの UDP パケットなどです。
ICMP	ICMP エコー要求（ping）を検出します。
IP	IP プロトコル スキャンを検出します。これらのスキャンは、攻撃者が開いているポートを見つけようとしているのではなく、ターゲット ホストでサポートされている IP プロトコルを発見しようとするためのスキャンであるため、TCP スキャンおよび UDP スキャンとは異なります。

（注）　イベントがポートスキャン接続ディテクタによって生成され場合、プロトコル番号は 255 に設定されます。デフォルトでは、ポートスキャンに特定のプロトコルは関連付けられません。したがって、Internet Assigned Numbers Authority（IANA）にはプロトコル番号が割り当てられません。IANA では 255 を予約番号として指定しているため、ポートスキャン イベントでは、そのイベントに関連付けられている番号がないことを示すために、この番号が使用されます。

一般に、ターゲット ホストの数、スキャン側ホストの数、およびスキャン対象のポートの数に応じて、ポートスキャンは 4 つのタイプに分けられます。以下の表に、検出できるポートスキャン アクティビティのタイプを記載します。

表 34-3　ポートスキャンのタイプ

タイプ（Type）	説明
ポートスキャン検出	1 対 1 のポートスキャン。攻撃者が 1 つまたは少数のホストを使用して、単一のターゲット ホスト上の複数のポートをスキャンする場合です。 1 対 1 の ポートスキャンには次のような特徴があります。 • 少数のホストを使用してスキャン • 単一のホストをスキャン • 多数のポートをスキャン このオプションでは、TCP、UDP、および IP ポートスキャンが検出されます。
ポートスイープ	1 対多のポートスイープ。攻撃者が 1 つまたは少数のホストを使用して、複数のターゲット ホスト上の単一のポートをスキャンする場合です。 ポートスイープには次のような特徴があります。 • 少数のホストを使用してスキャン • 多数のホストをスキャン • 少数の固有のポートをスキャン このオプションでは、TCP、UDP、ICMP、および IP ポートスイープが検出されます。
デコイ ポートスキャン	1 対 1 のポートスキャン。攻撃者がスプーフィングしたソース IP アドレスを実際のスキャン IP アドレスに混在させる場合です。 デコイ ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 少数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン デコイ ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。
分散型ポートスキャン	多対 1 のポートスキャン。複数のホストが単一のホストをクエリして開いているポートを調べる場合です。 分散型ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 多数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン 分散型ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。

ポートスキャン ディテクタは、主にプローブ対象ホストからの否定応答に基づいて、プローブに関する情報を取得します。たとえば、Web クライアントが Web サーバに接続するときに、クライアントはサーバのポート 80/tcp が開いていることを頼りに、そのポートを使用します。ただし、攻撃者がサーバを調査するとき、攻撃者には Web サービスが提供されているかどうか事前に分かりません。ポートスキャン ディテクタは否定応答（つまり、ICMP 到達不能または TCP RST パケット）を見つけると、その応答を潜在的ポートスキャンとして記録します。否定応答をフィルタリングするデバイス（ファイアウォールやルータなど）の向こう側にターゲット ホストがある場合、このプロセスはさらに困難になります。この場合、ポートスキャン ディテクタは、選択された機密レベルに基づいて *フィルタリングされた* ポートスキャン イベントを生成することができます。

以下の表に、選択可能な 3 つの機密レベルを記載します。

表 34-4　機密レベル

水準器	説明
低（Low）	ターゲット ホストからの否定応答だけが検出されます。誤検出を抑えるためには、この機密レベルを選択します。ただし、特定のタイプのポートスキャン（時間をかけたスキャン、フィルタリングされたスキャン）が見逃される可能性があることに注意してください。 このレベルを使用すると、ポートスキャン検出の所要時間が最短になります。
中（Medium）	ホストへの接続数に基づいてポートスキャンが検出されます。したがって、フィルタリングされたポートスキャンを検出できます。ただし、ネットワーク アドレス変換プログラムやプロキシなど、ホストが非常にアクティブな場合は、誤検出が発生する可能性があります。 [スキャン済みの無視（Ignore Scanned）] フィールドに、アクティブなホストの IP アドレスを追加すると、そのような誤検出を軽減できます。 このレベルを使用すると、ポートスキャン検出の所要時間が長くなります。
高（High）	期間に基づいてポートスキャンが検出されます。したがって、時間ベースのポートスキャンを検出できます。ただし、このオプションを使用する場合は、[スキャン済みの無視（Ignore Scanned）] および [スキャナの無視（Ignore Scanner）] フィールドに IP アドレスを指定するという方法で、時間をかけて慎重にディテクタを調整してください。 このレベルを使用すると、ポートスキャン検出の所要時間が大幅に長くなります。

詳細については、次の各項を参照してください。

- ポートスキャン検出の設定（34-5 ページ）
- ポートスキャン イベントについて（34-7 ページ）

ポートスキャン検出の設定

ライセンス：Protection

ポートスキャン検出の設定オプションを使用して、ポートスキャン ディテクタによるスキャン アクティビティのレポート方法を微調整できます。

ポートスキャン検出が有効になっていても、[ルール（Rules）] ページでジェネレータ ID（GID）が 122 に設定されたルールを有効にしなければ、ポートスキャン ディテクタの有効になっているポートスキャン タイプがポートスキャン イベントを生成しないことに注意してください。詳細については、ルール状態の設定（32-23 ページ）とポートスキャン検出 SID（GID:122）の表を参照してください。

ポートスキャン検出を設定する方法:

Admin/Intrusion Admin

手順 1　[ポリシー(Policies)] > [アクセス制御(Access Control)] > [アクセス コントロール ポリシー(Access Control Policy)] を選択して [アクセス コントロール ポリシー(Access Control Policy)] ページを表示し、[ネットワーク分析ポリシー(Network Analysis Policy)] をクリックします。

[ネットワーク分析ポリシー(Network Analysis 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。別のポリシーで保存されていない変更内容を保存する詳細については、[was Committing Intrusion Policy Changes; update xref] 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　左側のナビゲーション パネルで [設定(Settings)] をクリックします。

[設定(Settings)] ページが表示されます。

手順 4　[特定の脅威検知(Specific Threat Detection)] の [ポートスキャン検出(Portscan Detection)] が有効になっているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

  [ポートスキャン検出(Portscan Detection)] 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階層を示します。詳細については、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。

手順 5　[プロトコル(Protocol)] フィールドに、以下のプロトコルのうち、有効にするプロトコルを指定します。

- TCP
- UDP
- ICMP
- IP

Ctrl キーまたは Shift キーを押しながらクリックすることによって複数のプロトコルを選択するか、個々のプロトコルをクリアします。詳細については、プロトコル タイプの表を参照してください。

TCP を介してスキャンを検出するには TCP ストリーム処理が有効になっていること、UDP を介してスキャンを検出するには UDP ストリーム処理が有効になっていることが必要です。

手順 6　[スキャン タイプ(Scan Type)] フィールドに、以下の中から検出対象のポートスキャンを指定します。

- ポートスキャン検出
- ポートスイープ
- デコイ ポートスキャン
- 分散型ポートスキャン

複数のプロトコルを選択または選択解除するには、Ctrl キーまたは Shift キーを押しながらクリックします。詳細については、ポートスキャンのタイプ の表を参照してください。

手順 7　[機密レベル(Sensitivity Level)] リストで、使用するレベル(低、中、または高)を選択します。

詳細については、機密レベルの表を参照してください。

手順 8　オプションで、[IP の監視（Watch IP）] フィールドに、ポートスキャン アクティビティの兆候を監視するホストを指定します。すべてのネットワーク トラフィックを監視する場合は、このフィールドを空白のままにします。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-24 ページ）を参照してください。

手順 9　オプションで、[スキャナの無視（Ignore Scanners）] フィールドに、スキャナとして無視するホストを指定します。ネットワーク上で特にアクティブになっていないホストを指定するには、このフィールドを使用します。このホスト リストは、時間経過とともに変更しなければならない場合があります。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-24 ページ）を参照してください。

手順 10　オプションで、[スキャン済みの無視（Ignore Scanned）] フィールドに、スキャンのターゲットとして無視するホストを指定します。ネットワーク上で特にアクティブになっていないホストを指定するには、このフィールドを使用します。このホスト リストは、時間経過とともに変更しなければならない場合があります。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-24 ページ）を参照してください。

手順 11　オプションで、ミッドストリームで取得されたセッションのモニタを中断する場合は、[ACK スキャンの検出（Detect Ack Scans）] チェックボックスをオフにします。

（注）　ミッドストリーム セッションの検出は ACK スキャンの識別に役立ちますが、過大トラフィックで大量のパケットがドロップされるネットワークでは、誤ったイベントが生成されがちです。

手順 12　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。

ポートスキャン イベントについて

ライセンス：Protection

ポートスキャン検出が有効になっていても、ジェネレータ ID（GID）122 と Snort® ID（SID）1 ～ 27 のどれかが設定されたルールを有効にしなければ、有効にした各ポートスキャン タイプのイベントは生成されません。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。以下の表の「プリプロセッサ ルール SID」列に、各ポートスキャン タイプに対して有効にする必要があるプリプロセッサ ルールの SID をリストします。

表 34-5　ポートスキャン検出 SID（GID:122）

ポートスキャン タイプ	[プロトコル（Protocol）]:	機密レベル	プリプロセッサ ルール SID
ポートスキャン検出	TCP	低（Low）	1
		中または高	5
	UDP	低（Low）	17
		中または高	21
	ICMP	低（Low）	イベントを生成しません。
		中または高	イベントを生成しません。
	IP	低（Low）	9
		中または高	13
ポートスイープ	TCP	低（Low）	3、27
		中または高	7
	UDP	低（Low）	19
		中または高	23
	ICMP	低（Low）	25
		中または高	26
	IP	低（Low）	11
		中または高	15
デコイ ポートスキャン	TCP	低（Low）	2
		中または高	6
	UDP	低（Low）	18
		中または高	22
	ICMP	低（Low）	イベントを生成しません。
		中または高	イベントを生成しません。
	IP	低（Low）	10
		中または高	18
分散型ポートスキャン	TCP	低（Low）	4
		中または高	8
	UDP	低（Low）	20
		中または高	24
	ICMP	低（Low）	イベントを生成しません。
		中または高	イベントを生成しません。
	IP	低（Low）	12
		中または高	16

関連するプリプロセッサ ルールを有効にすると、ポートスキャン ディテクタによって侵入イベントが生成されるようになります。生成されたイベントは、他のすべての侵入イベントと同じように表示できます。ただし、ポートスキャン イベントのパケット ビューに表示される情報は、他のタイプの侵入イベントとは異なります。ここでは、ポートスキャン イベントのパケット ビューに表示されるフィールドと、これらのフィールドの情報を使用してネットワークで行われたプローブのタイプを把握する方法を説明します。

侵入イベント ビューを出発点に、ポートスキャン イベントのパケット ビューまでドリルダウンします。それには、侵入イベントの操作（41-1 ページ）の手順を使用できます。

各ポートスキャン イベントは複数のパケットに基づくため、単一のポートスキャン パケットをダウンロードすることはできません。ただし、ポートスキャン パケット ビューで、使用可能なすべてのパケット情報を確認できます。

(注)　イベントがポートスキャン接続ディテクタによって生成され場合、プロトコル番号は 255 に設定されます。デフォルトでは、ポートスキャンに特定のプロトコルは関連付けられません。したがって、Internet Assigned Numbers Authority（IANA）にはプロトコル番号が割り当てられません。IANA では 255 を予約番号として指定しているため、ポートスキャン イベントでは、そのイベントに関連付けられている番号がないことを示すために、この番号が使用されます。

以下の表に、ポートスキャン イベントのパケット ビューに表示される情報を記載します。任意の IP アドレスをクリックしてコンテキスト メニューを表示し、[whois] を選択して、その IP アドレスに関するルックアップを実行するか、[ホスト プロファイルの表示（View Host Profile）] を選択して、そのホストのホスト プロファイルを表示できます。

表 34-6　ポートスキャン パケット ビュー

情報	説明
Device	イベントを検出したデバイス。
時刻（Time）	イベントが発生した時刻。
メッセージ（Message）	プリプロセッサによって生成されたイベント メッセージ。
ソース IP	スキャン側ホストの IP アドレス。
宛先 IP（Destination IP）	スキャンされたホストの IP アドレス。
プライオリティ カウント（Priority Count）	スキャンされたホストからの否定応答（TCP RST、ICMP 到達不能など）の数。否定応答の数が多ければ多いほど、プライオリティ カウントが高くなります。
接続数（Connection Count）	ホスト上でアクティブな接続数。この値は、TCP や IP などの接続ベースのスキャンより正確です。
IP カウント（IP Count）	スキャン対象のホストに接続する IP アドレスが変更された回数。たとえば、最初の IP アドレスが 10.1.1.1、2 番目の IP アドレスが 10.1.1.2、3 番目の IP アドレスが 10.1.1.1 の場合、IP カウントは 3 となります。 プロキシや DNS サーバなどのアクティブ ホストでは、この数値はそれほど正確ではありません。
スキャナ/スキャン対象 IP 範囲（Scanner/Scanned IP Range）	スキャン対象ホストまたはスキャン側ホスト（スキャンのタイプに依存）の IP アドレスの範囲。ポートスイープの場合、このフィールドにはスキャン対象ホストの IP アドレス範囲が示されます。ポートスキャンの場合は、スキャン側ホストの IP アドレス範囲が示されます。
ポート/プロトコル カウント（Port/Proto Count）	TCP および UDP ポートスキャンの場合は、スキャン対象のポートが変更された回数です。たとえば、スキャンされた最初のポートが 80、2 番目のポートが 8080、3 番目のポートが再び 80 の場合、ポート カウントは 3 となります。 IP プロトコル ポートスキャンの場合は、スキャン対象ホストに接続するために使用されたプロトコルが変更された回数です。
ポート/プロトコル範囲（Port/Proto Range）	TCP および UDP ポートスキャンの場合は、スキャンされたポートの範囲です。 IP プロトコル ポートスキャンの場合は、スキャン対象ホストへの接続試行で使用された IP プロトコル番号の範囲です。
開いているポート（Open Ports）	スキャン対象ホストで開かれた TCP ポート。このフィールドは、ポートスキャンで 1 つ以上の開かれたポートが検出された場合にのみ表示されます。

レート ベース攻撃の防止

ライセンス：Protection

レート ベース攻撃とは、接続の頻度または攻撃を行うための反復試行に依存する攻撃のことです。レート ベースの検出基準を使用することで、レート ベース攻撃が行われていることを検出し、攻撃が発生するごとに対応できます。また、攻撃が収まった後は、通常の検出設定に戻すことができます。レート ベースの検出を設定する方法の詳細については、以下のトピックを参照してください。

- レート ベース攻撃の防止について（34-10 ページ）
- レート ベース攻撃防止とその他のフィルタ（34-13 ページ）
- レート ベース攻撃防止の設定（34-18 ページ）
- 動的ルール状態について（32-34 ページ）
- 動的ルール状態の設定（32-36 ページ）

レート ベース攻撃の防止について

ライセンス：Protection

レート ベース フィルタを含めたネットワーク分析ポリシーを設定することで、ネットワーク上のホストを対象とした過剰なアクティビティを検出できます。インライン モードで展開されている管理対象デバイスでこの機能を使用すると、指定の期間だけレートベース攻撃をブロックした後、イベントの生成だけを行ってトラフィックをドロップしない状態に戻せます。

レート ベースの攻撃防御は、異常なトラフィック パターンを識別し、正規の要求に対するそのトラフィックの影響を最小限に抑えようとします。一般に、レート ベース攻撃には次のいずれかの特性があります。

- 任意のトラフィックで、ネットワーク上のホストに対して過剰な未完了接続が発生する。これは、SYN フラッド攻撃を意味します。

  SYN 攻撃の検出を設定するには、SYN 攻撃の防止（34-12 ページ）を参照してください。

- 任意のトラフィックで、ネットワーク上のホストに対して過剰な接続が発生する。これは、TCP/IP 接続フラッド攻撃を意味します。

  同時接続の検出を設定するには、同時接続の制御（34-12 ページ）を参照してください。

- 1 つ以上の特定の宛先 IP アドレスへのトラフィック、または 1 つ以上の特定の送信元 IP アドレスからのトラフィックで、ルールとの一致が過剰に発生する。

  送信元または宛先ベースの動的ルール状態を設定するには、動的ルール状態の設定（32-36 ページ）を参照してください。

- すべてのトラフィックで、特定のルールとの一致が過剰に発生する。

  ルール ベースの動的ルール状態を設定するには、動的ルール状態の設定（32-36 ページ）を参照してください。

ネットワーク分析ポリシーでは、ポリシー全体に対して SYN フラッドまたは TCP/IP 接続フラッドの検出を設定できます。侵入ポリシーでは、個々の侵入ルールまたはプリプロセッサ ルールに対してレート ベース フィルタを設定できます。ルール 135:1 および 135:2 に手動でレート ベース フィルタを追加しても、効果はありません。GID:135 のルールでは、クライアントを送信元の値、サーバを宛先の値として使用します。詳細については、「SYN 攻撃の防止（34-12 ページ）」と「同時接続の制御（34-12 ページ）」を参照してください。

各レート ベース フィルタには、以下のコンポーネントが含まれます。

- ポリシー全体またはルール ベースの送信元/宛先の設定の場合、ネットワーク アドレスの指定
- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率
- レートを超過した場合に実行する新しいアクション

  ポリシー全体に対してレート ベースを設定すると、システムはレート ベース攻撃を検出した時点でイベントを生成します。インライン導入では、オプションでトラフィックをドロップすることもできます。個々のルールにレート ベース アクションを設定する場合は、[イベントを生成する（Generate Events）]、[ドロップしてイベントを生成する（Drop and Generate Events）]、[無効にする（Disable）] の 3 つのうちから選択できます。
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウト期間が満了し、レートがしきい値を下回っている場合、ルールのアクションはそのルールに最初に設定されたアクションに戻ります。ポリシー全体に適用される設定の場合、アクションは、トラフィックと一致する個々のルールのアクションに戻ります。一致するアクションがなければ、アクションは停止されます。

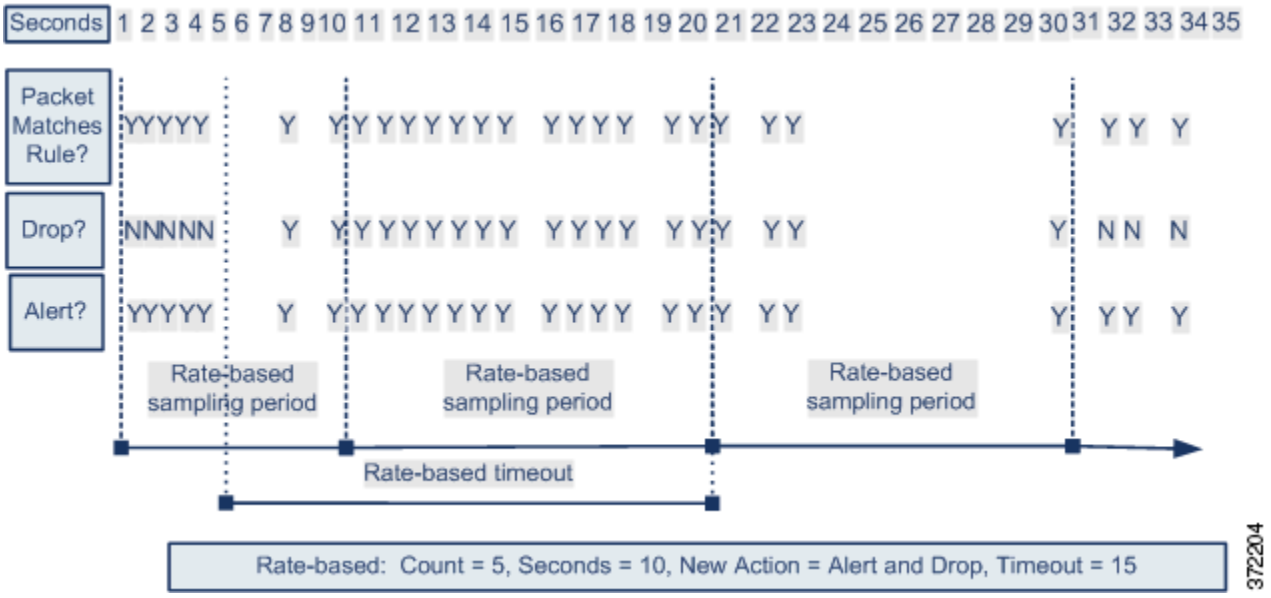
インライン展開のレート ベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レート ベースの設定が使用されていない場合、ルールが [イベントを生成する（Generate Events）] に設定されていればイベントが生成されますが、パケットがドロップされることはありません。ただし、攻撃トラフィックが、レート ベースの基準が設定されたルールと一致した場合は、そのようなルールが最初から [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていなかったとしても、レート アクションがアクティブな期間にパケットのドロップが実行されます。

（注） レート ベースのアクションは、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。ただし、ポリシー レベルでレート ベース フィルタを設定すると、指定した期間内の過剰な数の SYN パケットまたは SYN/ACK インタラクションを含むトラフィックに対してイベントを生成するか、イベントを生成してトラフィックをドロップすることができます。

同じルールに対して複数のレート ベースのフィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレート ベース フィルタ アクションが競合する場合は、最初のレート ベース フィルタのアクションが実行されることに注意してください。同様に、ポリシー全体に対するレート ベース フィルタと個々のルールに設定されたレート ベース フィルタが競合する場合は、ポリシー全体のレート ベース フィルタが優先されます。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。パスワードを検出しようとする試行が繰り返されると、レート ベース攻撃防止が設定されたルールがトリガーされます。レート ベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [ドロップしてイベントを生成する（Drop and Generate Events）] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または過去のサンプリング期間のしきい値を上回っている場合は、新しいアクションが継続されます。新しいアクションが元の「イベントの生成」アクションに戻されるのは、サンプリング期間の完了時にサンプルリング レートがしきい値を下回っている場合のみです。



SYN 攻撃の防止

ライセンス：Protection

ネットワークのホストを SYN フラッドから保護するには、SYN 攻撃防止オプションを利用します。一定期間中に認められたパケットの数を基準に、個々のホストまたはネットワーク全体を保護することができます。パッシブ導入のデバイスでは、イベントを生成できます。インライン導入のデバイスでは、不正なパケットをドロップすることもできます。タイムアウト期間の満了時にレート条件に達しなくなっていれば、イベントの生成およびパケットのドロップが停止します。

たとえば、1 つの IP アドレスからの SYN パケットの最大許容数を 10 に設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

このオプションを有効にすると、ルール 135:1 もアクティブになります。このルールを手動でアクティブにしても効果はありません。ルール状態は常に [無効（Disabled）] として表示され、変更されることはありません。このオプションを有効にすると、定義されたレート条件を超過した時点で、ルールによってイベントが生成されます。

同時接続の制御

ライセンス：Protection

ネットワーク上のホストでの TCP/IP 接続数を制限することで、サービス妨害（DoS）攻撃や、ユーザによる過剰なアクティビティを防止できます。システムが、指定の IP アドレスまたはアドレス範囲で正常に行われている接続が設定された許容数に達したことを検出すると、以降の接続に対してイベントを生成します。タイムアウト期間が満了するまでは、レート条件に達しなくなっても、レート ベースのイベント生成が続行されます。インライン導入では、レート条件がタイムアウトになるまでパケットをドロップするように設定できます。

たとえば、1 つの IP アドレスからの同時接続の最大許容数を 10 に設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

このオプションを有効にすると、ルール 135:2 もアクティブになります。このルールを手動でアクティブにしても効果はありません。ルール状態は常に [無効（Disabled）] として表示され、変更されることはありません。このオプションを有効にすると、定義されたレート条件を超過した時点で、ルールによってイベントが生成されます。

レート ベース攻撃防止とその他のフィルタ

ライセンス：Protection

トラフィック自体またはシステムが生成するイベントをフィルタリングする手段としては、`detection_filter` キーワード、しきい値および抑制機能も使用できます。レート ベース攻撃防止は、単独で使用することも、しきい値構成、抑制、または `detection_filter` キーワードと任意に組み合わせて使用することもできます。

詳細については、以下の例を参照してください。

- レート ベース攻撃防止と検出フィルタリング（34-13 ページ）
- 動的ルール状態としきい値または抑制（34-14 ページ）
- ポリシー全体のレート ベース検出としきい値構成または抑制（34-16 ページ）
- 複数のフィルタリング方法によるレート ベース検出（34-17 ページ）

レート ベース攻撃防止と検出フィルタリング

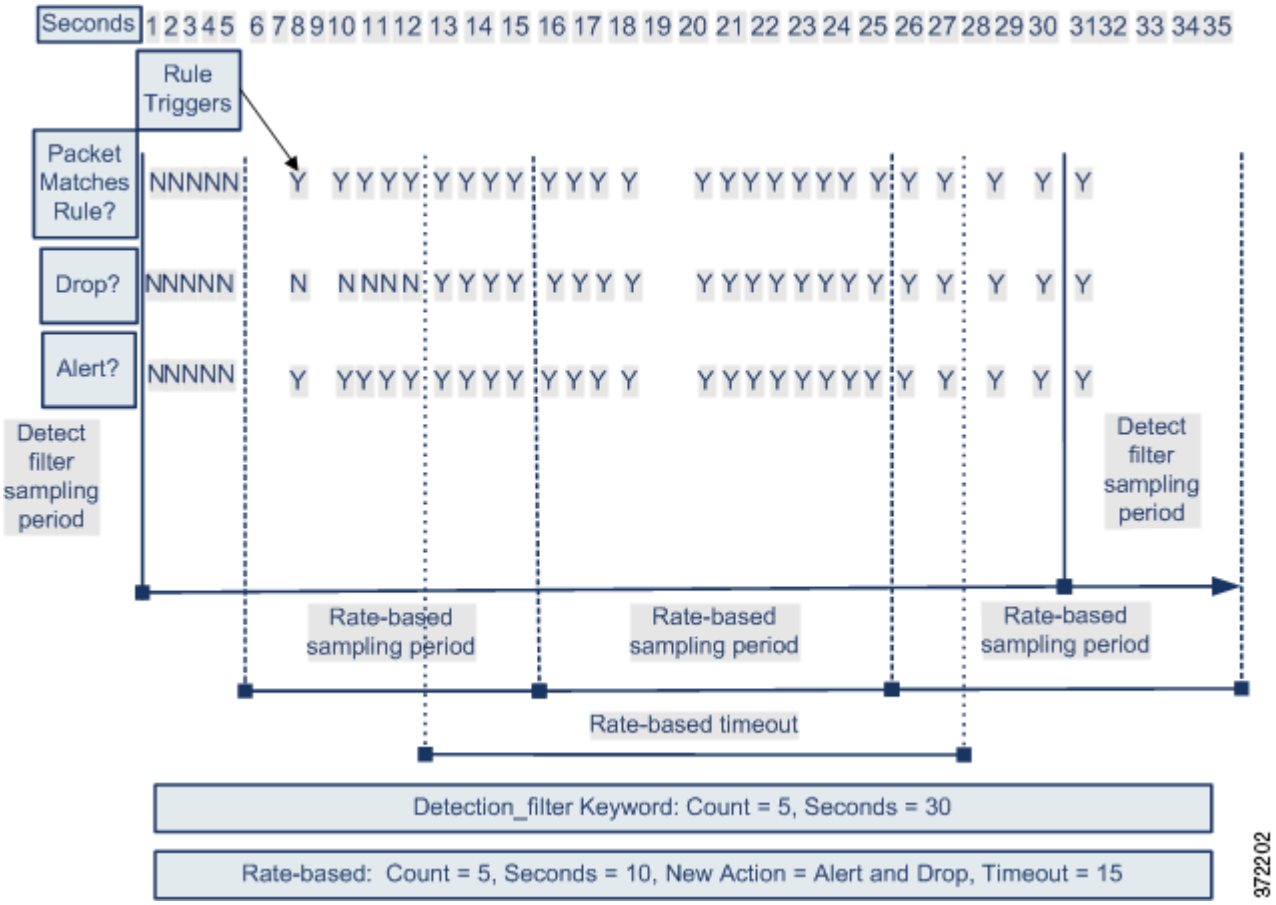
ライセンス：Protection

`detection_filter` キーワードを使用すると、指定の期間内にルール一致のしきい値に達するまで、ルールはトリガーされません。ルールに `detection_filter` キーワードが含まれている場合、システムは指定の期間、ルールのパターンに一致する着信パケットの数を追跡します。システムはそのルールについて、特定の送信元 IP アドレスからのヒット数、または特定の宛先 IP アドレスからのヒット数をカウントできます。レートがルールのレートを超過すると、そのルールに関するイベント通知が開始されます。

以下に、攻撃者がブルートフォース ログインを仕掛ける例を示します。パスワードの検出試行が繰り返されると、カウントが 5 に設定された `detection_filter` キーワードも含むルールがトリガーされます。このルールには、レート ベース攻撃防止が設定されています。10 秒以内にルールに 5 回ヒットすると、レート ベースの設定により、ルール属性が 20 秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。

図に示されているように、最初の 5 個のパケットがルールに一致しても、イベントは生成されません。それは、レートが `detection_filter` キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに 5 個のパケットが通過するまでは、レート ベースの基準によって新しいルールとして [ドロップしてイベントを生成する（Drop and Generate Events）] がトリガーされることはありません。

レート ベースの基準に一致すると、イベントが生成されて、パケットがドロップされます。これは、レート ベースのタイムアウト期間が満了し、かつレートがしきい値未満になるまで続きます。20 秒が経過すると、レート ベース アクションがタイムアウトになります。タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。タイムアウトが発生した時点で、サンプリングされたレートは前のサンプリング期間のしきい値レートを超過しているため、レート ベースのアクションは続行されます。



この例には示されていませんが、[ドロップしてイベントを生成する（Drop and Generate Events）] ルール状態を `detection_filter` キーワードと組み合わせて使用することで、ルールのヒット数が指定のレートに達するとトラフィックのドロップが開始されるようにすることができることにも注意してください。ルールにレート ベースの設定を使用するかどうかを決定する際は、ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定した場合の結果と `detection_filter` キーワードを含めた場合の結果が同じであるかどうか、あるいは侵入ポリシーでレートとタイムアウトの設定を管理する必要があるかどうかを検討してください。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。

動的ルール状態としきい値または抑制

ライセンス：Protection

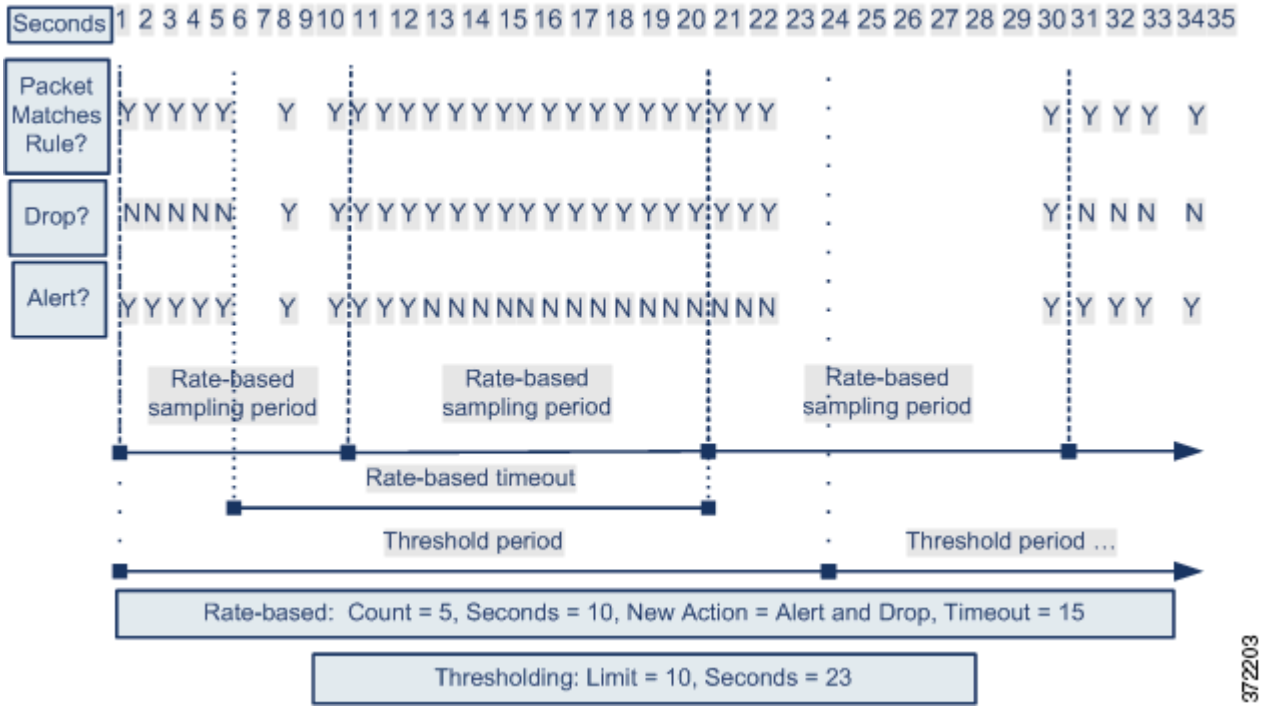
しきい値および抑制を使用して、ルールに関するイベント通知の数を制限するか、またはイベント通知を一切抑制することにより、過剰なイベントが生成されないようにすることができます。しきい値と抑制で使用可能なオプションの詳細については、イベントしきい値の設定（32-26 ページ）および侵入ポリシー単位の抑制の設定（32-31 ページ）を参照してください。

抑制をルールに適用すると、システムは、レート ベースのアクションが変更されたとしても、そのルールに関するイベント通知を、該当するすべての IP アドレスに対して抑制します。一方、しきい値とレート ベースの基準との間の相互作用はさらに複雑になります。

以下に、攻撃者がブルートフォース ログインを仕掛ける例を示します。パスワードを検出しようとする試行が繰り返されると、レート ベース攻撃防止が設定されたルールがトリガーされます。10 秒以内にルールに 5 回ヒットすると、レート ベースの設定により、ルール属性が 15 秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。さらに、上限しきい値により、ルールで生成可能なイベントの数が 23 秒間で 10 に制限されます。

図に示されているように、最初の 5 個のパケットが一致すると、ルールはイベントを生成します。5 個のパケットがルールに一致した後、レート ベースの基準が新しいアクションとして [ドロップしてイベントを生成する（Drop and Generate Events）] をトリガーし、次の 5 個のパケットがルールに一致した時点でイベントが生成され、パケットをドロップします。10 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成することなくドロップします。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが続行されます。新しいアクションが元の [イベントを生成する（Generate Events）] アクションに戻されるのは、サンプリング期間の完了時にサンプルリング レートがしきい値を下回っている場合のみです。



この例には示されていませんが、しきい値に達した*後に*、レート ベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の 10 に達してシステムがイベントの生成を停止し、14 番目のパケットでアクションが [イベントを生成する（Generate Events）] から [ドロップしてイベントを生成する（Drop and Generate Events）] に変更されると、システムはアクションが変更されたことを示す 11 番目のイベントを生成します。

ポリシー全体のレート ベース検出としきい値構成または抑制

ライセンス：Protection

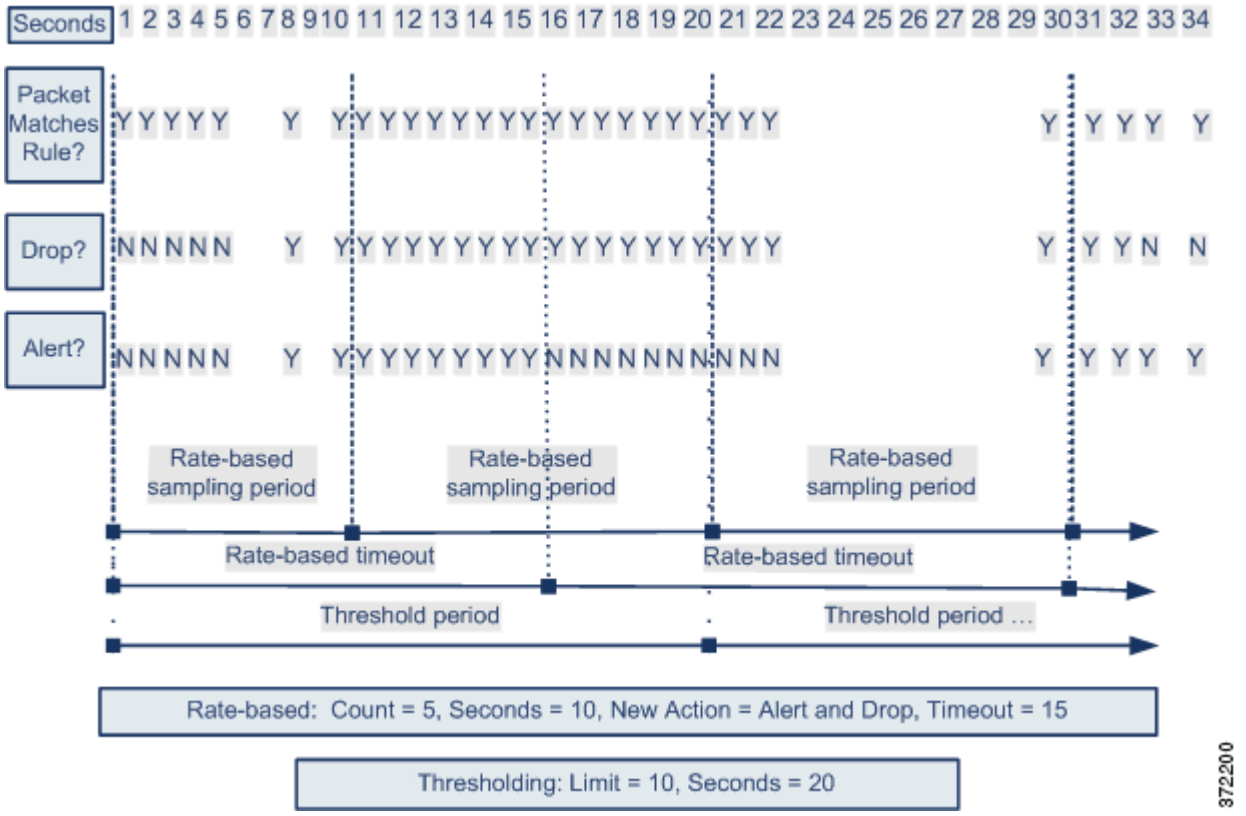
しきい値および抑制を使用して、送信元または宛先に関するイベント通知の数を制限するか、またはイベント通知を一切抑制することにより、過剰なイベントが生成されないようにすることができます。しきい値と抑制で使用可能なオプションの詳細については、グローバルしきい値の設定（35-3 ページ）、イベントしきい値の設定（32-26 ページ）、および侵入ポリシー単位の抑制の設定（32-31 ページ）を参照してください。

抑制がルールに適用されている場合、ポリシー全体またはルール固有のレート ベースの設定によって、レート ベースのアクションが変更されたとしても、該当するすべての IP アドレスに対してそのルールに関するイベント通知が抑制されます。一方、しきい値とレート ベースの基準との間の相互作用はさらに複雑になります。

以下に、ネットワーク上のホストに対して、攻撃者がサービス妨害（DoS）攻撃を仕掛ける例を示します。同じ送信元から多数のホストに対して同時接続が行われると、ポリシー全体の [同時接続の制御（Control Simultaneous Connections）] 設定がトリガーされます。この設定は、1 つの送信元からの接続数が 10 秒間で 5 つに達すると、イベントを生成して悪意のあるトラフィックをドロップします。さらに、グローバル上限しきい値により、ルールまたは設定で生成可能なイベントの数が 20 秒間で 10 件に制限されます。

この図に示されているように、ポリシー全体の設定により、一致する最初の 10 個のパケットに対してイベントが生成され、トラフィックがドロップされます。10 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリングされたレートが、現在または前のサンプリング期間のしきい値レートを超過している場合、レート ベースのアクションによるイベントの生成とトラフィックのドロップが続行されます。レート ベース アクションが停止するのは、サンプリング期間が完了した時点で、サンプリングされたレートがしきい値レートを下回っている場合のみです。



この例には示されていませんが、しきい値に達した*後に*、レート ベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の 10 に達してシステムがイベントの生成を停止し、14 番目のパケットでアクションが [ドロップしてイベントを生成する（Drop and Generate Events）] に変更されると、システムはアクションが変更されたことを示す 11 番目のイベントを生成します。

複数のフィルタリング方法によるレート ベース検出

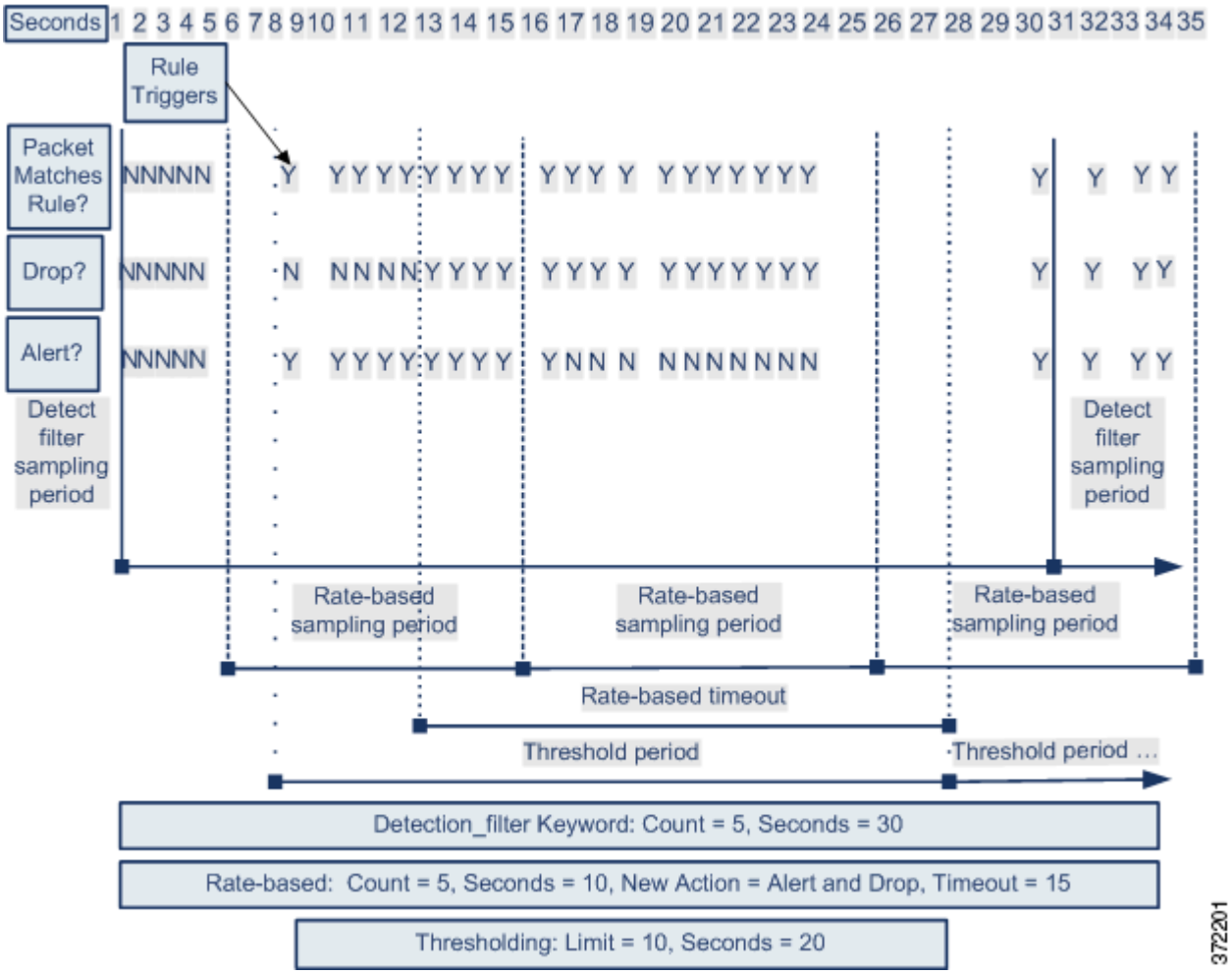
ライセンス：Protection

`detection_filter` キーワード、しきい値構成または抑制、およびレート ベースの基準のすべてが同じトラフィックに適用されるという状況が発生することもあります。抑制をルールに適用すると、レート ベースの変更が発生しても、指定の IP アドレスに対するイベントの生成は抑制されます。

以下に、攻撃者がブルートフォース ログインを仕掛ける例で、`detection_filter` キーワード、レート ベースのフィルタリング、およびしきい値が相互作用する場合を説明します。パスワードの検出試行が繰り返されると、カウントが 5 に設定された `detection_filter` キーワードを含むルールがトリガーされます。このルールには、レート ベース攻撃防止も設定されています。その設定では、15 秒間にルールのヒット数が 5 に達すると、ルール属性が 30 秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。さらに、上限しきい値により、ルールによって生成されるイベントは 30 秒間で 10 件に制限されます。

図に示されているように、最初の 5 個のパケットがルールに一致しても、イベント通知は行われません。それは、detection_filter キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに 5 個のパケットが通過するまでは、レート ベースの基準によって新しいルールとして [ドロップしてイベントを生成する(Drop and Generate Events)] がトリガーされることはありません。レート ベースの基準が満たされると、システムは 11 個目から 15 個目のパケットに対してイベントを生成し、パケットをドロップします。15 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

レート ベースのタイムアウトが発生した後は、それに続くレート ベースのサンプリング期間中、パケットが引き続きドロップされることに注意してください。サンプリング レートが前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが続行されます。



レート ベース攻撃防止の設定

ライセンス: Protection

ポリシー レベルでレート ベース攻撃防止を設定することで、SYN フラッド攻撃を阻止できます。特定の送信元からの過剰な接続、または特定の宛先への過剰な接続を阻止することもできます。

レート ベース攻撃防止の設定方法:

Admin/Intrusion Admin

手順 1　[ポリシー(Policies)] > [アクセス制御(Access Control)] > [アクセス コントロール ポリシー(Access Control Policy)] を選択して [アクセス コントロール ポリシー(Access Control Policy)] ページを表示し、[ネットワーク分析ポリシー(Network Analysis Policy)] をクリックします。

[ネットワーク分析ポリシー(Network Analysis 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　左側のナビゲーション パネルで [設定(Settings)] をクリックします。

[設定(Settings)] ページが表示されます。

手順 4　[特定の脅威検知(Specific Threat Detection)] の下にある [レート ベース攻撃の防止(Rate-Based Attack Prevention)] が有効になっているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[レート ベース攻撃の防止(Rate-Based Attack Prevention)] 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階層を示します。詳細については、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。

手順 5　次の 2 つの対処法があります。

- ホストのフラッディングを目的とする不完全な接続を防ぐには、[SYN 攻撃の防止(SYN Attack Prevention)] の下にある [追加(Add)] をクリックします。

  [SYN 攻撃の防止(SYN Attack Prevention)] ダイアログボックスが表示されます。
- 過剰な数の接続を防ぐには、[同時接続の制御(Control Simultaneous Connections)] の下にある [追加(Add)] をクリックします。

  [同時接続の制御(Control Simultaneous Connections)] ダイアログボックスが表示されます。

手順 6　トラフィックを追跡する方法を選択します。

- 特定の送信元または送信元の範囲からのすべてのトラフィックを追跡するには、[追跡対象(Track By)] ドロップダウンリストから [送信元(Source)] を選択し、[ネットワーク(Network)] フィールドに単一の IP アドレスまたはアドレス ブロックを入力します。
- 特定の宛先または宛先の範囲へのすべてのトラフィックを追跡するには、[追跡対象(Track By)] ドロップダウンリストから [宛先(Destination)] を選択し、[ネットワーク(Network)] フィールドに単一の IP アドレスまたはアドレス ブロックを入力します。

システムは、[ネットワーク(Network)] フィールドに含まれる各 IP アドレスのトラフィックを個別に追跡することに注意してください。ある特定の IP アドレスからの設定されたレートを超過するトラフィックがある場合、その IP アドレスに関するイベントだけが生成されることになります。例として、ネットワーク設定で `10.1.0.0/16` の送信元 CIDR ブロックを設定し、10 個の同時接続が開始された時点でイベントを生成するようにシステムを設定するとします。10.1.4.21 から 8 つの接続が開始され、10.1.5.10 から 6 つの接続が開始されている場合、いずれの送信元も開始されている接続がトリガーを引き起こす数になっていないため、システムはイベントを生成しません。一方、10.1.4.21 から 11 個の同時接続が開始されている場合、システムは 10.1.4.21 からの接続に対してだけイベントを生成します。

FireSIGHT システムで CIDR 表記およびプレフィクス長を使用する方法の詳細については、IP アドレスの表記規則（1-24 ページ）を参照してください。

手順 7　レート追跡設定をトリガーとして使用するレートを指定します。

- SYN 攻撃に対する設定の場合は、[レート（Rate）] フィールドに、一定の秒数あたりの SYN パケット数を指定します。
- 同時接続に対する設定の場合は、[カウント（Count）] フィールドに、接続数を指定します。

手順 8　レート ベース攻撃防止設定に一致するパケットをドロップするには、[ドロップ（Drop）] を選択します。

手順 9　[タイムアウト（Timeout）] フィールドに、イベント生成のタイムアウト期間を指定します。この期間を経過すると、SYN または同時接続のパターンに一致するトラフィックに対するイベント生成が（該当する場合はドロップも）停止されます。

注意　タイムアウト値には 1 ～ 1,000,000 の整数を指定できます。ただし、インライン導入では、大きいタイムアウト値を指定するとホストへの接続が完全にブロックされる可能性があります。

手順 10　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。

センシティブ データの検出

ライセンス：Protection

社会保障番号、クレジット カード番号、運転免許証番号などのセンシティブ データは、インターネットに意図的に、または誤って漏洩される可能性があります。システムには、ASCII テキストのセンシティブ データに関するイベントを検出し、生成できるセンシティブ データ プロセッサが用意されています。このプロセッサは、特に誤って漏洩されたデータの検出に役立ちます。

このシステムは、暗号化または難読化されたセンシティブ データ、あるいは圧縮または符号化された形式のセンシティブ データ（たとえば、Base64 でエンコードされた電子メールの添付ファイルなど）の検出は行いません。たとえば、システムは電話番号 (555)123-4567 を検出しますが、(5 5 5) 1 2 3 - 4 5 6 7 のようにスペースで難読化されたバージョン、あるいは (555)-123-4567 のように HTML コードが介在するバージョンは検出しません。ただし、(555)-123-4567 のように、HTML にコーディングされた番号のパターンの途中にコードが入っていなければ検出されます。

ヒント　センシティブ データ プリプロセッサでは、FTP または HTTP を使用してアップロードおよびダウンロードされる暗号化されていない Microsoft Word ファイル内のセンシティブ データを検出できます。これが可能である理由は、Word ファイルが ASCII テキストとフォーマット設定コマンドを分けてグループ化する方式だからです。

システムはトラフィックに対して個別のデータ タイプを照合することによって、TCP セッションごとにセンシティブ データを検出します。侵入ポリシーの、各データ タイプのデフォルト設定およびすべてのデータ タイプに適用されるグローバル オプションのデフォルト設定は変更できます。Cisco では、事前定義された、よく使用されるデータ タイプを用意しています。カスタム データ タイプを作成することも可能です。

センシティブ データのプリプロセッサ ルールは、各データ タイプに関連付けられます。各データ タイプのセンシティブ データ検出とイベント生成を有効にするには、そのデータ タイプに対応するプリプロセッサ ルールを有効にします。設定ページのリンクを使用すると、センシティブ データ ルールにフィルタリングされたビューが [ルール(Rules)] ページに表示されます。このビューで、ルールを有効または無効にしたり、その他のルール属性を設定したりできます。

変更を侵入ポリシーに保存する際に提示されるオプションによって、データ タイプに関連付けられたルールが有効になっていてセンシティブ データ検出が無効になっている場合には、自動的にセンシティブ データ プリプロセッサを有効にすることができます。

詳細については、次の各項を参照してください。

センシティブ データ検出の導入

ライセンス: Protection

センシティブ データ検出は FireSIGHT システムのパフォーマンスに非常に大きな影響を与える可能性があるため、Ciscoでは以下のガイドラインに従うことを推奨しています。

- デフォルト ポリシー No Rules Active をベースになる侵入ポリシーとして選択します。詳細については、システムによって提供される基本ポリシーについて(24-3 ページ)を参照してください。
- 次の設定が対応するネットワーク分析ポリシーで有効になっていることを確認します。
  - [アプリケーション層プリプロセッサ(Application Layer Preprocessors)] の下の [FTP と Telnet の構成(FTP and Telnet Configuration)]
  - [トランスポートまたはネットワーク レイヤ プロセッサ(Transport/Network Layer Preprocessors)] の下の [IP 最適化(IP Defragmentation)] および [TCP ストリームの構成(TCP Stream Configuration)]
- センシティブ データ設定のある侵入ポリシーを含むアクセス コントロール ポリシーは、センシティブ データ検出用に予約済みの別個のデバイスに適用します。詳細については、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。

グローバル センシティブ データ検出オプションの選択

ライセンス: Protection

グローバル センシティブ データ プリプロセッサ オプションは、プリプロセッサの動作を制御します。以下のことを指定するグローバル オプションを変更できます。

- プリプロセッサが、ルールをトリガーしたパケットで、クレジット カード番号または社会保障番号の下位 4 桁を除くすべての桁を置換するかどうか
- センシティブ データをモニタする、ネットワーク上の宛先ホスト
- イベントの生成基準となる、単一のセッションでの全データ タイプの合計オカレンス数

グローバル センシティブ データ オプションはポリシーに固有であり、すべてのデータ タイプに適用されることに注意してください。

次のグローバルなセンシティブ データ検出オプションを設定できます。

マスク（Mask）

ルールをトリガーしたパケットで、クレジット カード番号および社会保障番号の下位 4 桁を除くすべての桁を「X」に置換します。Web インターフェイスの侵入イベント パケット ビューおよびおよびダウンロードされたパケットでは、マスクされた番号が表示されます。詳細については、パケット ビューの使用（41-25 ページ）を参照してください。

ネットワーク

センシティブ データをモニタする 1 つ以上の宛先ホストを指定します。単一の IP アドレス、アドレス ブロック、あるいはこのいずれかまたは両方のカンマ区切りリストを指定できます。空白のフィールドは、any として解釈されます。これは、任意の宛先 IP アドレスを意味します。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-24 ページ）を参照してください。

グローバルしきい値（Global Threshold）

グローバルしきい値イベントの生成基準となる、単一セッションでの全データ タイプの合計オカレンス数を指定します。データ タイプの組み合わせを問わず、プリプロセッサは指定された数のデータ タイプを検出すると、グローバルしきい値イベントを生成します。1 ～ 65535 の値を指定できます。

Cisco では、このオプションに、ポリシーで有効にする個々のデータ タイプに対するしきい値のどれよりも大きい値を設定することを推奨しています。詳細については、個別データ タイプ オプションの選択（34-22 ページ）を参照してください。

グローバルしきい値については、以下の点に注意してください。

- 複数のデータ タイプを合わせたオカレンス数を検出してイベントを生成するには、プリプロセッサ ルールの 139:1 を有効にする必要があります。侵入ポリシーでルールを有効に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。
- プリプロセッサが生成するグローバルしきい値イベントは、セッションあたり最大 1 件です。
- グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立しています。つまり、グローバルしきい値に達すると、個別データ タイプに対するイベントしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も当てはまります。

個別データ タイプ オプションの選択

ライセンス：Protection

個別のデータ タイプによって、指定した宛先ネットワーク トラフィックで検出しイベントを生成できるセンシティブ データを特定します。以下のことを指定するデータ タイプ オプションのデフォルト設定を変更できます。

- 検出されたデータ タイプに対して単一のセッションごとのイベントを生成する基準とするしきい値
- 各データ タイプをモニタする宛先ポート
- 各データ タイプをモニタするアプリケーション プロトコル

最低でも、データ タイプごとにイベントしきい値を指定し、モニタする少なくとも 1 つのポートまたはアプリケーション プロトコルを指定する必要があります。

Cisco で用意している各定義済みデータ タイプでは、デフォルト値が変更されない限り、アクセス不能な `sd_pattern` キーワードを使用して、トラフィックで検出する組み込みデータ パターンを定義します。定義済みデータ タイプのリストについては、表 34-8（34-24 ページ）を参照してください。カスタム データ タイプを作成して、そのデータ タイプに対し、単純な正規表現を使用して独自のデータ パターンを指定することもできます。詳細については、カスタム データ タイプの使用（34-29 ページ）を参照してください。

データ タイプの名前とパターンはシステム全体に適用されることに注意してください。その他すべてのデータ タイプ オプションはポリシーに固有です。

次の表に、設定できるデータ タイプ オプションを記載します。

表 34-7　個別データ タイプ オプション

オプション	説明
データ タイプ	データ タイプの一意の名前を表示します。
しきい値（Threshold）	イベント生成の基準とする、データ タイプのオカレンス数を指定します。有効にしたデータ タイプに対してしきい値を設定せずにポリシーを保存しようとすると、エラー メッセージが表示されます。1 ～ 255 の値を指定できます。 プリプロセッサが検出したデータ タイプに対して生成するイベント数は、セッションごとに 1 つであることに注意してください。グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立していることにも注意してください。つまり、データ タイプ イベントしきい値に達すると、グローバルしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も当てはまります。
宛先ポート（Destination Ports）	データ タイプでモニタする宛先ポートを指定します。単一のポート、複数のポートをカンマで区切ったリスト、または任意の宛先ポートを意味する `any` を指定できます。データ タイプのルールを有効にした場合、そのデータ タイプに対して少なくとも 1 つのポートまたはアプリケーション プロトコルを設定せずにポリシーを保存しようとすると、エラー メッセージが表示されます。
アプリケーション プロトコル（Application Protocols） この機能には、Control ライセンスが必要です。	データ タイプでモニタする最大 8 つのアプリケーション プロトコルを指定します。データ タイプのルールを有効にした場合、そのデータ タイプに対して少なくとも 1 つのポートまたはアプリケーション プロトコルを設定せずにポリシーを保存しようとすると、エラー メッセージが表示されます。 選択するアプリケーション プロトコルごとに、少なくとも 1 つのディテクタを有効にする必要があります（ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照）。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。アプリケーション プロトコルに対して有効になっているディレクタがない場合は、Cisco 提供のすべてのディテクタがアプリケーションに対して自動的に有効になります。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタがアプリケーションに対して有効になります。 データ タイプのアプリケーション プロトコルを選択する方法の詳細については、モニタするアプリケーション プロトコルの選択（34-27 ページ）を参照してください。

表 34-7　個別データ タイプ オプション（続き）

オプション	説明
パターン	カスタム データ タイプの場合、検出するパターンを指定します（Cisco 提供のデータ タイプのデータ パターンは事前に定義されています）。詳細については、カスタム データ タイプの使用（34-29 ページ）を参照してください。Web インターフェイスには、定義済みデータ タイプの組み込みパターンは表示されません。 カスタム データ パターンと定義済みデータ パターンは、システム全体に適用されることに注意してください。

定義済みデータ タイプの使用

ライセンス：Protection

それぞれの侵入ポリシーには、よく使用されるデータ パターンを検出するために事前に定義されたデータ タイプが含まれています。これらのデータ パターンには、クレジット カード番号、電子メールアドレス、米国の電話番号、および米国の社会保障番号などがあります（番号にはハイフン付きのパターン、ハイフン抜きのパターンがあります）。各定義済みデータ タイプは、ジェネレータ ID（GID）が 138 に設定された単一のセンシティブ データ プリプロセッサに関連付けられます。ポリシーで使用する各データ タイプに対し、検出およびイベント生成を有効にするには、侵入ポリシーで関連付けられたセンシティブ データ ルールを有効にする必要があります。侵入ポリシーでルールを有効に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。

センシティブ データ ルールを有効にするには、設定ページに表示されるリンクを利用できます。このリンクを使用すると、すべての定義済みセンシティブ データ ルールおよびカスタム センシティブ データ ルールを表示するフィルタリングされたビューの [ルール（Rules）] ページが表示されます。また、センシティブ データ ルールのフィルタ カテゴリを選択して、[ルール（Rules）] ページに定義済みセンシティブ データ ルールだけを表示することもできます。詳細については、侵入ポリシー内のルールのフィルタリング（32-11 ページ）を参照してください。定義済みセンシティブ データ ルールは、[ルール エディタ（Rule Editor）] ページ（[ポリシー（Policies）] > [侵入（Intrusion）] > [ルール エディタ（Rule Editor）]）にもリストされます。このページでは、センシティブ データ ルール カテゴリに属する定義済みセンシティブ データ ルールを確認できますが、これらのルールを編集することはできません。

以下の表に、データ タイプを記載し、各データ タイプを検出してイベントを生成するために有効にしなければならない、対応するプリプロセッサ ルールをリストします。

表 34-8　センシティブ データ タイプ

データ タイプ	説明	プリプロセッサ ルール GID:SID
クレジット カード番号	Visa®、MasterCard®、Discover®、および American Express® の 15 桁または 16 桁のクレジット カード番号（通常の区切り文字として使用されるハイフンまたはスペースが含まれるパターンと含まれないパターン）に一致します。また、Luhn アルゴリズムを使用してクレジット カード番号の検査数字を確認します。	138:2
電子メール アドレス	電子メール アドレスに一致します。	138:5
米国の電話番号	米国の電話番号（`(\d\{3\}) ?\d\{3\}-\d\{4\}` のパターンに準拠）に一致します。	138:6

表 34-8　センシティブ データ タイプ(続き)

データ タイプ	説明	プリプロセッサ ルール GID:SID
米国の社会保障番号(ハイフンなし)	米国の 9 桁の社会保障番号(有効な 3 桁のエリア番号と有効な 2 桁のグループ番号が含まれ、ハイフンを使用していない番号)に一致します。	138:4
米国の社会保障番号(ハイフンあり)	米国の 9 桁の社会保障番号(有効な 3 桁のエリア番号と有効な 2 桁のグループ番号が含まれ、ハイフンを使用した番号)に一致します。	138:3
カスタム(Custom)	指定されたトラフィックでユーザ定義のデータ パターンに一致します。詳細については、カスタム データ タイプの使用(34-29 ページ)を参照してください。	138:>999999

社会保障番号以外の 9 桁の番号からの誤検出を軽減するために、プリプロセッサでは、各社会保障番号の 4 桁のシリアル番号の前にある 3 桁のエリア番号と 2 桁のグループ番号を検証するアルゴリズムを使用します。プリプロセッサは 2009 年 11 月末までの社会保障グループ番号を検証します。

センシティブ データ検出の設定

ライセンス: Protection

デフォルトのグローバル設定および個別データ タイプの設定を変更できます。検出する各データ タイプのプリプロセッサ ルールを有効にする必要もあります。

ポリシーでセンシティブ データ プリプロセッサ ルールを有効にして、センシティブ データ検出を有効にしていなければ、変更をポリシーに保存する際に、センシティブ データ検出を有効にするよう求めるプロンプトが出されます。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。

以下の表に、[センシティブ データの検出(Sensitive Data Detection)] ページで実行できる操作を記載します。

表 34-9　センシティブ データ設定の操作

目的	操作
グローバル設定を変更する	ユーザが変更できるグローバル設定については、表 34-6(34-9 ページ)を参照してください。
データ タイプ オプションを変更する	[ターゲット(Targets)] ページ領域で、データ タイプの名前をクリックします。 [設定(Configuration)] ページ領域が更新され、データ タイプの現在の設定が表示されます。ユーザが変更できるオプションについては、個別データ タイプ オプションの表を参照してください。

表 34-9　センシティブ データ設定の操作（続き）

目的	操作
データ タイプでモニタするアプリケーション プロトコルを追加または削除する この機能には、Control ライセンスが必要です。	[アプリケーション プロトコル（Application Protocols）] フィールド内をクリックするか、このフィールドの横にある [編集（Edit）] をクリックします。[アプリケーション プロトコル（Application Protocols）] ポップアップ ウィンドウが表示されます。 • モニタするアプリケーション プロトコル（最大 8 つ）を追加するには、左側の [選択可能（Available）] リストからアプリケーション プロトコルを 1 つ以上選択して、右矢印（>）ボタンをクリックします。 • アプリケーション プロトコルを削除するには、右側の [有効（Enabled）] リストから削除するアプリケーション プロトコルを選択して、左矢印（<）ボタンをクリックします。 複数のアプリケーション プロトコルを選択する場合は、Ctrl または Shift キーを押しながらクリックします。また、クリックしてドラッグすることによって、隣接する複数のアプリケーション プロトコルを選択することもできます。 選択するアプリケーション プロトコルごとに、少なくとも 1 つのディテクタを有効にする必要があります（ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照）。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。アプリケーション プロトコルに対して有効になっているディレクタがない場合は、Cisco 提供のすべてのディテクタがアプリケーションに対して自動的に有効になります。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタがアプリケーションに対して有効になります。 （注）　FTP トラフィックの機密データを検出するには、`Ftp data` アプリケーション プロトコルを追加する必要があります。詳細については、特殊な場合：FTP トラフィックでのセンシティブ データの検出（34-29 ページ）を参照してください。
カスタム データ タイプを作成する	ページ左側の [データ タイプ（Data Types）] の横にある [+] 記号をクリックします。[データ タイプの追加（Add Data Type）] ポップアップ ウィンドウが表示されます。 データ タイプの一意の名前と、このデータ タイプで検出するパターンを指定して、[OK] をクリックします。編集を破棄するには [キャンセル（Cancel）] をクリックします。詳細については、カスタム データ タイプの使用（34-29 ページ）を参照してください。
センシティブ データ プリプロセッサ ルールを表示する	[グローバル設定（Global Settings）] ページ領域の上に表示されている [センシティブ データ検出ルールの設定（Configure Rules for Sensitive Data Detection）] リンクをクリックします。[ルール（Rules）] ページの表示がフィルタリングされ、すべてのセンシティブ データ プリプロセッサ ルールのリストが表示されます。 オプションで、リストされているルールを有効または無効にすることができます。侵入ポリシーで使用する各データ タイプのセンシティブ データ プリプロセッサ ルールを有効に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、ルール状態の設定（32-23 ページ）を参照してください。 [ルール（Rules）] ページで使用可能なその他の操作（ルールの抑制、レート ベース攻撃の防止など）のセンシティブ データ ルールも設定できます。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。 [戻る（Back）] をクリックして [センシティブ データの検出（Sensitive Data Detection）] ページに戻ります。

センシティブ データ検出を設定する方法:

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　左側のナビゲーション パネルの [詳細設定(Advanced Settings)] をクリックします。

[詳細設定(Advanced Settings)] ページが表示されます。

手順 4　[特定の脅威検知(Specific Threat Detection)] の下にある [センシティブ データの検出(Sensitive Data Detection)] が有効になっているかどうかによって、2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[センシティブ データの検出(Sensitive Data Detection)] 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階層を示します。詳細については、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。

手順 5　センシティブ データ設定の操作の表で説明されている操作を実行できます。

手順 6　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。

モニタするアプリケーション プロトコルの選択

ライセンス: Control

各データ タイプでモニタするアプリケーション プロトコルを最大 8 つ指定できます。システムがネットワーク上で検出できるアプリケーション プロトコルの詳細については、サーバの使用(50-39 ページ)を参照してください。

選択するアプリケーション プロトコルごとに、少なくとも 1 つのディテクタを有効にする必要があります(ディテクタのアクティブ化と非アクティブ化(46-30 ページ)を参照)。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。アプリケーション プロトコルに対して有効になっているディレクタがない場合は、Cisco 提供のすべてのディテクタがアプリケーションに対して自動的に有効になります。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタがアプリケーションに対して有効になります。

各データ タイプをモニタするアプリケーション プロトコルまたはポートを少なくとも 1 つ指定する必要があります。ただし、FTP トラフィックでセンシティブ データを検出する場合を除き、Cisco では最も包括的なカバレッジにするために、アプリケーション プロトコルを指定する際には対応するポートを指定することを推奨しています。たとえば、HTTP を指定する場合は、既知の HTTP ポート 80 も設定します。このように設定すると、ネットワークの新しいホストが HTTP を実装する場合には、システムは新しい HTTP アプリケーション プロトコルを検出する間、ポート 80 をモニタします。

FTP トラフィックでセンシティブ データを検出する場合は、FTP data アプリケーション プロトコルを指定する必要があります。この場合、ポート番号を指定する利点はありません。詳細については、特殊な場合：FTP トラフィックでのセンシティブ データの検出（34-29 ページ）を参照してください。

センシティブ データを検出するためにアプリケーション プロトコルを変更する方法：

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　左側のナビゲーション パネルの [詳細設定（Advanced Settings）] をクリックします。

[詳細設定（Advanced Settings）] ページが表示されます。

手順 4　[特定の脅威検知（Specific Threat Detection）] の下にある [センシティブ データの検出（Sensitive Data Detection）] が有効になっているかどうかによって、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[センシティブ データの検出（Sensitive Data Detection）] 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階層を示します。詳細については、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。

手順 5　[データ タイプ（Data Types）] にリストされているデータ タイプ名をクリックして、変更するデータ タイプを選択します。

[設定（Configuration）] 領域が更新されて、選択したデータ タイプの現在の設定が表示されます。

手順 6　[アプリケーション プロトコル（Application Protocols）] フィールド内をクリックするか、このフィールドの横にある [編集（Edit）] をクリックします。

[アプリケーション プロトコル（Application Protocols）] ポップアップ ウィンドウが表示されます。

手順 7　次の 2 つの選択肢があります。

- モニタするアプリケーション プロトコル（最大 8 つ）を追加するには、左側の [選択可能（Available）] リストからアプリケーション プロトコルを 1 つ以上選択して、右矢印（>）ボタンをクリックします。
- アプリケーション プロトコルを削除するには、右側の [有効（Enabled）] リストから削除するアプリケーション プロトコルを選択して、左矢印（<）ボタンをクリックします。

複数のアプリケーション プロトコルを選択する場合は、Ctrl または Shift キーを押しながらクリックします。また、クリックしてドラッグすることによって、隣接する複数のアプリケーション プロトコルを選択することもできます。

（注）　FTP トラフィックの機密データを検出するには、FTP data アプリケーション プロトコルを追加する必要があります。詳細については、特殊な場合：FTP トラフィックでのセンシティブ データの検出（34-29 ページ）を参照してください。

手順 8　[OK] をクリックしてアプリケーション プロトコルを追加します。

[センシティブ データの検出(Sensitive Data Detection)] ページが表示され、アプリケーション プロトコルが更新されます。

特殊な場合:FTP トラフィックでのセンシティブ データの検出

ライセンス: Control

一般に、センシティブ データをモニタするトラフィックを決めるには、導入でのモニタ対象のポートを指定するか、あるいはオプションで、アプリケーション プロトコルを指定します。ただし、FTP トラフィックでセンシティブ データを検出するには、ポートまたはアプリケーション プロトコルを指定するだけでは不十分です。FTP トラフィックのセンシティブ データは、FTP アプリケーション プロトコルのトラフィックで検出されますが、FTP アプリケーション プロトコルは断続的に発生し、一時的なポート番号を使用するため、センシティブ データを検出するのが困難です。FTP トラフィックでセンシティブ データを検出するには、以下の設定を含めることが**必須**となります。

- `FTP data` アプリケーション プロトコルを指定します。

  `FTP data` アプリケーション プロトコルを指定すると、FTP トラフィックでのセンシティブ データの検出が可能になります。詳細については、モニタするアプリケーション プロトコルの選択(34-27 ページ)を参照してください。

  FTP トラフィックでセンシティブ データを検出するという特殊な場合では、`FTP data` アプリケーション プロトコルを指定すると、検出が呼び出される代わりに、FTP トラフィックでセンシティブ データを検出するために FTP/Telnet プロセッサの高速処理が呼び出されます。詳細については、FTP および Telnet トラフィックのデコード(27-20 ページ)を参照してください。

- FTP データ ディテクタが有効であることを確認します(デフォルトで有効にされます)。

  ディテクタのアクティブ化と非アクティブ化(46-30 ページ)を参照してください。

- 設定に、センシティブ データをモニタするポートが少なくとも 1 つ含まれていることを確認します。

  FTP トラフィックでセンシティブ データを検出することだけが目的の場合を除き(そのような場合はほとんどありません)、FTP ポートを指定する必要はありません。通常のセンシティブ データ設定には、HTTP ポートや電子メール ポートなどの他のポートが含まれることになります。モニタ対象の FTP ポートを 1 つだけ指定し、他のポートを指定しない場合、Cisco では、FTP コマンド ポート `23` を指定することを推奨しています。詳細については、センシティブ データ検出の設定(34-25 ページ)を参照してください。

カスタム データ タイプの使用

ライセンス: Protection

指定するデータ パターンを検出するためのカスタム データ タイプを作成および変更することができます。たとえば、病院で患者番号を保護するためのデータ タイプを作成したり、大学で固有の番号パターンを持つ学生番号を検出するためのデータ タイプを作成したりすることが考えられます。

作成するカスタム データ タイプごとに、単一のセンシティブ データ プリプロセッサ ルールも作成します。このルールのジェネレータ ID（GID）は 138 で、Snort ID は 1000000 以上（これは、ローカル ルールの SID）です。ポリシーで特定のデータ タイプを検出してイベントを生成するには、そのカスタム データ タイプに関連付けられたセンシティブ データ ルールを有効にする必要があります。侵入ポリシーでルールを有効に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。

センシティブ データ ルールを有効にするには、設定ページに表示されるリンクを利用できます。このリンクを使用すると、すべての定義済みセンシティブ データ ルールおよびカスタム センシティブ データ ルールを表示するフィルタリングされたビューの [ルール（Rules）] ページが表示されます。また、ローカル ルールのフィルタ カテゴリを選択して、[ルール（Rules）] ページにカスタム センシティブ データ ルールだけを表示することもできます。詳細については、侵入ポリシー内のルールのフィルタリング（32-11 ページ）を参照してください。カスタム センシティブ データ ルールは、[ルール エディタ（Rule Editor）] ページには表示されないことに注意してください。

作成するカスタム データ タイプは、すべての侵入ポリシーに追加されます。特定のカスタム データ タイプを検出してイベントを生成するには、使用するポリシーで、そのカスタム データ タイプに関連付けられたセンシティブ データ ルールを有効にする必要があります。

データ タイプとそのデータ タイプに関連付けるルールを作成するには、[センシティブ データの検出（Sensitive Data Detection）] 設定ページを使用する必要があることに注意してください。ルール エディタを使用してセンシティブ データ ルールを作成することはできません。

詳細については、次の各項を参照してください。

- カスタム データ タイプのデータ パターンの定義（34-30 ページ）
- カスタム データ タイプの設定（34-32 ページ）
- カスタム データ タイプの名前と検出パターンの編集（34-34 ページ）

カスタム データ タイプのデータ パターンの定義

ライセンス：Protection

カスタム データ タイプのデータ パターンを定義するには、以下の要素からなる単純な正規表現のセットを使用します。

- 3 つのメタ文字
- メタ文字をリテラル文字として使用するためのエスケープ文字
- 6 文字クラス

メタ文字は正規表現内で特別な意味を持つリテラル文字です。以下の表に、カスタム データ パターンを定義する際に使用できるメタ文字を記載します。

表 34-10　センシティブ データ パターンのメタ文字

メタ文字	説明	例
?	先行する文字またはエスケープ シーケンスのゼロまたは 1 つのオカレンスに一致します。つまり、先行する文字またはエスケープ シーケンスはオプションです。	colou?r は、color または colour に一致します。
{*n*}	先行する文字またはエスケープ シーケンスの *n* 回の繰り返しに一致します。	次の例を参考にしてください。 \d{2} は、55、12 などに一致します。 \l{3} は、AbC、www などに一致します。 \w{3} は、a1B、25C などに一致します。 x{5} は、xxxxx に一致します。
\	メタ文字を実際の文字として使用できます。また、事前定義された文字クラスを指定するためにも使われます。センシティブ データ パターンで使用できる文字クラスについては、表 34-12（34-31 ページ）を参照してください。	\? は疑問符に一致します。 \\ はバックスラッシュに一致します。 \d は数字に一致します。

以下の表に記載する文字をリテラル文字としてセンシティブ データ プリプロセッサに正しく解釈させるには、バックスラッシュで文字をエスケープする必要があります。

表 34-11　センシティブ データ パターンのエスケープ文字

使用するエスケープ文字	表現されるリテラル文字
\?	?
\{	{
\}	}
\\	\

以下の表に、カスタム センシティブ データ パターンを定義する際に使用できる文字クラスを記載します。

表 34-12　センシティブ データ パターンの文字クラス

文字クラス	説明	文字クラスの定義
\d	ASCII 文字の数字 0 ～ 9 に一致します。	0 ～ 9
\D	ASCII 文字の数字ではないバイトに一致します。	0 ～ 9 以外
\l（小文字の「エル」）	任意の ASCII 文字に一致します。	a-zA-Z
\L	ASCII 文字ではないバイトに一致します。	a-zA-Z 以外

表 34-12　センシティブ データ パターンの文字クラス（続き）

文字クラス	説明	文字クラスの定義
\w	任意の ASCII 英数字に一致します。 PCRE 正規表現とは異なり、アンダースコア（_）は含まれないことに注意してください。	a-zA-Z0-9
\W	ASCII 英数字でないバイトに一致します。	a-zA-Z0-9 以外

プリプロセッサは、そのまま入力された文字を、正規表現の一部ではなく、リテラル文字として扱います。たとえば、データ パターン 1234 は `1234` に一致します。

以下に、定義済みセンシティブ データ ルール 138:4 で使用するデータ パターンの例を示します。このパターンでは、エスケープされた数値の文字クラス、複数個を示すメタ文字およびオプション指定子のメタ文字、リテラル ハイフン（-）文字、および左右の括弧 () 文字を使用して、米国の電話番号を検出します。

```
(\d{3}) ?\d{3}-\d{4}
```

カスタム データ パターンを作成する際には注意が必要です。以下に、電話番号を検出するための別のデータ パターンを示します。このパターンでは有効な構文を使用しているものの、多数の誤検出が発生する可能性があります。

```
(?\d{3})? ?\d{3}-?\d{4}
```

上記の 2 番目の例では、オプションの括弧、オプションのスペース、オプションのハイフンを組み合わせているため、目的とする以下のパターンの電話番号が検出されます。

- `(555)123-4567`
- `555123-4567`
- `5551234567`

ただし、2 番目の例のパターンでは、以下の潜在的に無効なパターンも検出されて、結果的に誤検出となります。

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

最後に、説明目的の極端な例として、小規模な企業ネットワーク上のすべての宛先トラフィックで小さいイベントしきい値を使用して、小文字の `a` を検出するデータ パターンを作成するとします。このようなデータ パターンは、わずか数分で文字通り数百万ものイベントを生成することになり、システムを過負荷に陥らせる可能性があります。

カスタム データ タイプの設定

ライセンス：Protection

基本的には、カスタム データ タイプにも、定義済みデータ タイプを設定する場合と同じデータ タイプ オプションを設定します。すべてのデータ タイプに共通の設定オプションを設定する方法については、個別データ タイプ オプションの選択（34-22 ページ）を参照してください。また、カスタム データ タイプにも名前とデータ パターンを指定する必要があります。

カスタム データ タイプを作成すると、そのカスタム データ タイプに関連付けられたカスタム センシティブ データ プリプロセッサ ルールが作成されます。このルールは、カスタム データ タイプを使用する各ポリシーで有効にしなければならないことに注意してください。侵入ポリシーでルールを有効に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。

カスタム データ タイプを作成または変更する方法:

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　左側のナビゲーション パネルの [詳細設定(Advanced Settings)] をクリックします。

[詳細設定(Advanced Settings)] ページが表示されます。

手順 4　[特定の脅威検知(Specific Threat Detection)] の下にある [センシティブ データの検出(Sensitive Data Detection)] が有効になっているかどうかによって、2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[センシティブ データの検出(Sensitive Data Detection)] 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階層を示します。詳細については、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。

手順 5　次の選択肢があります。

- カスタム データ タイプを作成するには、ページ左側の [データ タイプ(Data Types)] の横にある [+] 記号をクリックします。[データ タイプの追加(Add Data Type)] ポップアップ ウィンドウが表示されます。

  データ タイプの一意の名前と、このデータ タイプで検出するパターンを指定して、[OK] をクリックします。編集を破棄するには [キャンセル(Cancel)] をクリックします。詳細については、カスタム データ タイプの名前と検出パターンの編集(34-34 ページ)を参照してください。

  [センシティブ データの検出(Sensitive Data Detection)] ページが表示されます。[OK] をクリックすると、ページが更新されて変更が反映されます。

- 定義済みデータ タイプとカスタム データ タイプに共通のオプションを変更するには、[ターゲット(Targets)] ページ領域でデータ タイプ名をクリックします。

  [設定(Configuration)] ページ領域が更新され、データ タイプの現在の設定が表示されます。詳細については、センシティブ データ検出の設定(34-25 ページ)を参照してください。

- システム全体に適用されるカスタム データ タイプの名前およびデータ パターンを編集するには、カスタム データ タイプの名前と検出パターンの編集(34-34 ページ)を参照してください。

- カスタム データ タイプを削除するには、削除するデータ タイプの横にある削除アイコン( )をクリックしてから、[OK] をクリックします。データ タイプの削除を中止する場合は、[キャンセル(Cancel)] をクリックします。

  データ タイプのセンシティブ データ ルールがいずれかの侵入ポリシーで有効にされている場合、そのデータ タイプを削除することはできません。カスタム データ タイプを削除すると、そのカスタム データ タイプはすべての侵入ポリシーから削除されます。

カスタム データ タイプの名前と検出パターンの編集

ライセンス：Protection

システム全体に適用されるカスタム センシティブ データ ルールの名前および検出パターンを変更できます。これらの設定を変更すると、システム上の他のすべてのポリシーに変更が適用されます。変更したカスタム データ タイプを使用する侵入ポリシーが含まれるアクセス コントロール ポリシーを再適用する必要があることにも注意してください。

カスタム データ タイプの名前とデータ パターンを除き、カスタム データ タイプと定義済みデータ タイプのすべてのデータ タイプ オプションは、ポリシーに固有です。カスタム データ タイプで名前とデータ パターンを除くオプションを変更する方法については、個別データ タイプ オプションの選択（34-22 ページ）を参照してください。

カスタム データ タイプの名前およびデータ パターンを編集する方法：

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　左側のナビゲーション パネルの [詳細設定（Advanced Settings）] をクリックします。

[詳細設定（Advanced Settings）] ページが表示されます。

手順 4　[特定の脅威検知（Specific Threat Detection）] の下にある [センシティブ データの検出（Sensitive Data Detection）] が有効になっているかどうかによって、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[センシティブ データの検出（Sensitive Data Detection）] 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階層を示します。詳細については、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。

手順 5　[ターゲット（Targets）] ページ領域で、変更するカスタム データ タイプの名前をクリックします。

ページが更新されて、データ タイプの現在の設定が表示されます。また、[設定（Configuration）] ページ領域の右上隅に、[データ タイプの名前およびパターンの編集（Edit Data Type Name and Pattern）] リンクが表示されます。

手順 6　[データ タイプの名前およびパターンの編集（Edit Data Type Name and Pattern）] リンクをクリックします。

[データ タイプの編集（Edit Data Type）] ポップアップ ウィンドウが表示されます。

手順 7　データ タイプの名前、パターン、またはその両方を変更して、[OK] をクリックします。編集を破棄する場合は、[キャンセル（Cancel）] をクリックします。データ パターンを指定する方法については、カスタム データ タイプのデータ パターンの定義（34-30 ページ）を参照してください。

[センシティブ データの検出（Sensitive Data Detection）] ページが表示されます。[OK] をクリックすると、ページに変更が反映されます。
