侵入イベントの操作

FireSIGHT システムは、ホストとそのデータの可用性、整合性、および機密性に影響する可能性のあるトラフィックがないかどうか、ネットワークをモニタするのに役立ちます。主要なネットワーク セグメントに管理対象デバイスを配置すると、悪意のあるアクティビティを目的としてネットワークを通過するパケットを検査できます。このシステムには、攻撃者が開発したさまざまなエクスプロイトを検索するのに使用できるいくつかのメカニズムがあります。

システムは、潜在的な侵入を特定すると*侵入イベント*を生成します。これは、エクスプロイトの日付、時間、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報の記録です。パケットベースのイベントの場合、イベントをトリガーしたパケットのコピーも記録されます。管理対象デバイスは、防御センター にイベントを送信します。ここで、集約データを確認し、ネットワーク アセットに対する攻撃をより的確に把握できます。

管理対象デバイスをインライン型、スイッチ型、またはルート型の侵入システムとして展開することもできます。これにより、危険だと認識したパケットをドロップまたは置換するようデバイスを設定できます。

FireSIGHT システムは、ユーザが侵入イベントを確認し、ネットワーク環境とセキュリティ ポリシーのコンテキストでそのイベントが重要であるかどうかを評価するために必要なツールを提供します。これらのツールは次のとおりです。

- 管理対象デバイスでの現在のアクティビティの概要について説明するイベント サマリー ページ
- 選択した任意の期間に対して生成できるテキストベースおよびグラフィカルなレポート。独自のレポートを設計し、スケジュールされた間隔で実行されるよう設定することもできます
- 攻撃に関連したイベント データの収集に使用できるインシデント処理ツール。調査や応答のトラッキングに役立つ注記を追加することもできます
- SNMP、電子メール、および Syslog で設定できる自動アラート
- 特定の侵入イベントに対する応答や修復に使用できる自動化された相関ポリシー
- データをドリルダウンして、さらに調査したいイベントを特定するのに使用できる定義済みカスタム ワークフロー

詳細については、次の各項を参照してください。

- 侵入イベントの統計の表示（41-2 ページ）では [侵入イベント統計（Intrusion Event Statistics）] ページについて説明しています。このページでは、アプライアンスのヘルスの概要とネットワークに対する上位の脅威の要約について説明します。
- 侵入イベントのパフォーマンスの表示（41-5 ページ）では、侵入イベントのパフォーマンス統計情報のグラフを生成する方法について説明します。
- 侵入イベント グラフの表示（41-10 ページ）では、経時的にイベントのトレンドを示すグラフを生成する方法について説明します。

- 侵入イベントの表示（41-10 ページ）では、Web インターフェイスを使用して侵入イベントを表示および調査する方法について説明します。
- 侵入イベントのワークフロー ページについて（41-20 ページ）では、侵入イベント ワークフローで使用可能なさまざまなページと、それらを使用して侵入イベントを分析する方法について説明します。
- ドリルダウン ページとテーブル ビュー ページの使用（41-21 ページ）では、侵入イベント ワークフローでの 2 つのタイプのページの機能について説明します。
- パケット ビューの使用（41-25 ページ）では、侵入イベントのパケット ビューの使用方法について説明します。
- 影響レベルを使用してイベントを評価する（41-41 ページ）では、影響レベルを使用して侵入イベントを評価する方法について説明します。
- プリプロセッサ イベントの読み取り（41-43 ページ）では、プリプロセッサ ルールによって生成されるイベントを読み取る方法について説明します。
- 侵入イベントの検索（41-46 ページ）では、検索機能を使用して侵入イベントのリストを特定の条件に制限する方法について説明します。
- クリップボードの使用（41-54 ページ）では、後でイベントをインシデントに追加できるように、クリップボードと呼ばれる保存エリアに侵入イベントを追加する方法について説明します。この項では、クリップボードの内容に基づいてイベント レポートを生成する方法についても説明します。

次の項も参照してください。

- インシデント対応（42-1 ページ）では、インシデント処理についての詳細と、インシデントを使用してイベント分析の進行状況をトラックする方法について説明します。
- 侵入ルールの外部アラートの設定（44-1 ページ）では、自動アラートの詳細について説明します。
- レポートの操作（57-1 ページ）では、侵入イベントのレポートの詳細について説明します。
- 地理位置情報の使用（58-24 ページ）では、侵入イベントの地理位置情報の詳細について説明します。

侵入イベントの統計の表示

ライセンス：Protection

[侵入イベント統計（Intrusion Event Statistics）] ページは、アプライアンスの現在の状態の概要と、ネットワークで生成されたすべての侵入イベントを表示します。

[侵入イベント統計（Intrusion Event Statistics）] ページには、次の 3 つのメイン エリアがあります。

- ホスト統計情報（41-3 ページ）では、[ホスト統計（Host Statistics）] セクションについて説明します。このセクションは、アプライアンスに関する情報、および、防御センター の場合はその管理対象デバイスに関する情報を表示します。
- イベントの概要（41-4 ページ）では、イベント データベース情報の概要を表示する [イベントの概要（Event Overview）] について説明します。
- イベント統計情報（41-4 ページ）では、上位 10 件のイベント タイプなど、イベント データベースの情報の詳細を具体的に表示する [イベント統計（Event Statistics）] について説明します。

このページの IP アドレス、ポート、プロトコル、イベント メッセージなどはそれぞれリンクになっています。関連イベントの情報を表示するには、任意のリンクをクリックします。たとえば、上位 10 個の宛先ポートのいずれかが 80(http)/tcp である場合、そのリンクをクリックすると、デフォルトの侵入イベント ワークフローの最初のページが表示され、そのポートをターゲットとするイベントがリストされます。現在の時刻範囲で表示されるのはイベント（およびイベントを生成する管理対象デバイス）のみであることに注意してください。さらに、確認済みマークを付けた侵入イベントも統計に引き続き表示されます。たとえば、現在の時刻範囲が過去 1 時間であり、最初のイベントが 5 時間前に生成された場合、[最初のイベント（First Event）] リンクをクリックすると、そのイベントは時刻範囲を変更するまでイベント ページには表示されません。

侵入イベントの統計情報を表示する方法:

アクセス: Admin/Intrusion Admin

手順 1　[概要（Overview）] > [概要（Summary）] > [侵入イベント統計（Intrusion Event Statistics）] を選択します。

[侵入イベント統計（Intrusion Event Statistics）] ページが表示されます。

手順 2　ページの上部にある 2 つの選択ボックスから、統計を表示するゾーンおよびデバイスを選択するか、[すべてのセキュリティ ゾーン（All Security Zones）] および [すべてのデバイス（All Devices）] を選択して、侵入イベントを収集するすべてのデバイスの統計を表示します。

手順 3　[統計の取得（Get Statistics）] をクリックします。

[侵入イベント統計（Intrusion Event Statistics）] ページは、選択したデバイスのデータに表示が更新されます。

ヒント　カスタム時刻範囲からデータを表示するには、右上のページ エリアのリンクをクリックし、イベント時間の制約の設定（58-27 ページ）にある指示に従います。

手順 4　[侵入イベント統計（Intrusion Event Statistics）] ページで表示される統計の詳細については、次のセクションを参照してください。

- ホスト統計情報（41-3 ページ）
- イベントの概要（41-4 ページ）
- イベント統計情報（41-4 ページ）

ホスト統計情報

ライセンス: Protection

[侵入イベント統計（Intrusion Event Statistics）] ページの [ホスト統計（Host Statistics）] セクションは、アプライアンス自体に関する情報を提供します。防御センター では、このセクションはすべての管理対象デバイスに関する情報も提供します。

この情報には、次の内容が含まれます。

- [時間（Time）] は、アプライアンス上の現在の時刻を表示します。
- [稼働時間（Uptime）] は、アプライアンス自体が再起動してから経過した日数、時間、および分数を示します。防御センター では、[稼働時間（Uptime）] に各管理対象デバイスの最終起動時刻、ログインしたユーザの数、および負荷平均も示されます。

- [ディスク使用率(Disk Usage)] は、使用中のディスクのパーセンテージを示します。
- [メモリ使用率(Memory Usage)] は、使用中のシステム メモリのパーセンテージを示します。
- [負荷平均(Load Average)] は、過去 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数を示します。

イベントの概要

ライセンス: Protection

[侵入イベント統計(Intrusion Event Statistics)] ページの [イベントの概要(Event Overview)] セクションは、侵入イベント データベースにある情報の概要を示します。

これらの統計には、次が含まれています。

- [イベント(Events)] は、侵入イベント データベース内のイベント数を示します。
- [時間範囲内のイベント(Events in Time Range)] は、現在選択されている時間範囲と、時間範囲内に収まるデータベースのイベント数とパーセンテージを示します。
- [最初のイベント(First Event)] は、イベント データベース内の最初のイベントのイベント メッセージを示します。
- [最終イベント(Last Event)] は、イベント データベース内の最後のイベントのイベント メッセージを示します。

(注) 防御センター では、管理対象デバイスを選択した場合、そのデバイスの [イベントの概要(Event Overview)] セクションが代わりに表示されることに注意してください。

イベント統計情報

ライセンス: Protection

[侵入イベント統計(Intrusion Event Statistics)] ページの [イベント統計(Event Statistics)] セクションでは、侵入イベント データベース内の情報に関する具体的な情報が表示されます。

この情報には、次に関する詳細が含まれます。

- 上位 10 個のイベント タイプ
- 上位 10 個の送信元 IP アドレス
- 上位 10 個の宛先 IP アドレス
- 上位 10 個の宛先ポート
- イベント数が最大であるプロトコル、入力と出力のセキュリティ ゾーン、およびデバイス

侵入イベントのパフォーマンスの表示

ライセンス：Protection

[侵入イベント パフォーマンス（Intrusion Event Performance）] ページでは、指定された期間の侵入イベントのパフォーマンス統計情報を示すグラフを生成できます。グラフを生成することにより、1 秒あたりの侵入イベントの数、1 秒あたりのメガビット数、1 パケットあたりの平均バイト数、Snort によって検査されていないパケットの割合、および TCP 正規化の結果としてブロックされたパケットの数を反映できます。これらのグラフは、過去 1 時間、前日、先週、または先月の操作の統計を表示できます。

詳細については、侵入イベントのパフォーマンス統計グラフの生成（41-5 ページ）を参照してください。

侵入イベントのパフォーマンス統計情報を表示する方法：

アクセス：Admin/Maint

手順 1　[概要（Overview）] > [概要（Summary）] > [侵入イベント パフォーマンス（Intrusion Event Performance）] を選択します。

[侵入イベント パフォーマンス（Intrusion Event Performance）] ページが表示されます。

侵入イベントのパフォーマンス統計グラフの生成

ライセンス：Protection

1 秒あたりのイベント数、1 秒あたりのメガビット数、1 パケットあたりの平均バイト数、Snort によって検査されていないパケットの割合、および TCP 正規化の結果としてブロックされたパケット数に基づいて、防御センター または管理対象デバイスのパフォーマンス統計を示すグラフを生成できます。

（注）　新しいデータは 5 分ごとに統計グラフに蓄積されます。したがって、グラフをすぐにリロードしても、次の 5 分の差分更新が実行されるまでデータは変更されていない場合があります。

次の表に、表示可能なグラフの種類を示します。ネットワーク分析ポリシーの [インライン モード（Inline Mode）] 設定の影響を受けるデータを含むグラフ タイプでは、表示が異なるので注意してください。[インライン モード（Inline Mode）] が無効になっている場合、Web インターフェイスでアスタリスク（*）が付いているグラフ タイプ（下記の表では列に `Yes` と記載）には、[インライン モード（Inline Mode）] が有効になっている場合に変更またはドロップされるトラフィックに関するデータが含まれています。[インライン モード（Inline Mode）] 設定の詳細については、インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（26-6 ページ）を参照してください。

必須のオプションと設定の詳細については、インライン トラフィックの正規化（29-7 ページ）、インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（26-6 ページ）、およびインライン展開でのドロップ動作の設定（31-6 ページ）を参照してください。

表 41-1　侵入イベントのパフォーマンス グラフの種類

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
平均バイト/パケット	適用対象外	各パケットに含まれる平均バイト数。	No
TCP トラフィックまたはパケットで正規化された ECN フラグ	[明示的輻輳通知（Explicit Congestion Notification）] を有効にして、[パケット（Packet）] を選択します。	ネゴシエーションに関係なく、パケット単位で ECN フラグがクリアされたパケットの数。	Yes
TCP トラフィックまたはセッションで正規化された ECN フラグ	[明示的輻輳通知（Explicit Congestion Notification）] を有効にして、[ストリーム（Stream）] を選択します。	ECN の使用がネゴシエートされなかった場合にストリーム単位で ECN フラグがクリアされた回数。	Yes
イベント/秒	適用対象外	デバイスで生成された 1 秒あたりのイベント数。	No
ICMPv4 エコーの正規化	[ICMPv4 の正規化（Normalize ICMPv4）] を有効にします。	エコー（要求）またはエコー応答メッセージの 8 ビット コード フィールドがクリアされた ICMPv4 パケットの数。	Yes
ICMPv6 エコーの正規化	[ICMPv6 の正規化（Normalize ICMPv6）] を有効にします。	エコー（要求）またはエコー応答メッセージの 8 ビット コード フィールドがクリアされた ICMPv6 パケットの数。	Yes
IPv4 DF フラグの正規化	[IPv4 の正規化（Normalize IPv4）] と [DF ビットの正規化（Normalize Don’t Fragment Bit）] を有効にします。	IPv4 フラグ ヘッダー フィールドのシングル ビット DF（Don’t Fragment）サブフィールドがクリアされた IPv4 パケットの数。	Yes
IPv4 オプションの正規化	[IPv4 の正規化（Normalize IPv4）] を有効にします。	オプション オクテットが 1（No Operation）に設定された IPv4 パケットの数。	Yes
IPv4 予約済みフラグの正規化	[IPv4 の正規化（Normalize IPv4）] と [予約済みビットの正規化（Normalize Reserved Bit）] を有効にします。	IPv4 フラグ ヘッダー フィールドのシングル ビット予約済みサブフィールドがクリアされた IPv4 パケットの数。	Yes
IPv4 サイズ変更の正規化	[IPv4 の正規化（Normalize IPv4）] を有効にします。	超過ペイロードが IP ヘッダーで指定されたデータグラム長に切り詰められた IPv4 パケットの数。	Yes
IPv4 TOS の正規化	[IPv4 の正規化（Normalize IPv4）] と [TOS ビットの正規化（Normalize TOS Bit）] を有効にします。	1 バイト差別化サービス（DS）フィールド（旧「タイプ オブ サービス（ToS）フィールド」）がクリアされた IPv4 パケットの数。	Yes
IPv4 TTL の正規化	[IPv4 の正規化（Normalize IPv4）]、[最大 TTL（Maximum TTL）]、および [TTL のリセット（Reset TTL）] を有効にします。	IPv4 存続時間（TTL）正規化の数。	Yes

表 41-1　侵入イベントのパフォーマンス グラフの種類(続き)

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
IPv6 オプションの正規化	[IPv6 の正規化(Normalize IPv6)] を有効にします。	ホップバイホップ オプションまたは宛先オプション拡張ヘッダーのオプション タイプ フィールドが、00(スキップして処理を続行)に設定された IPv6 パケットの数。	Yes
IPv6 TTL の正規化	[IPv6 の正規化(Normalize IPv6)]、[最小 TTL(Minimum TTL)]、および [TTL のリセット(Reset TTL)] を有効にします。	IPv6 ホップ リミット(TTL)正規化の数。	Yes
メガビット/秒	適用対象外	デバイスをパス スルーするトラフィックの 1 秒あたりのメガビット数。	No
MSS に合わせてサイズ変更されたパケットの正規化	[データを MSS にトリミング(Trim Data to MSS)] を有効にします。	ペイロードが TCP データフィールドよりも長かったために、ペイロードが最大セグメント サイズに切り詰められたパケットの数。	Yes
TCP ウィンドウに合わせてサイズ変更されたパケットの正規化	[データをウィンドウにトリミング(Trim Data to Window)] を有効にします。	受信側ホストの TCP ウィンドウに合わせて TCP データフィールドが切り詰められたパケットの数。	Yes
ドロップされたパケットの割合	適用対象外	選択されたすべてのデバイスにおける未検査のパケットの平均パーセンテージ。たとえば、2 つのデバイスを選択した場合、平均が 50 % であるというのは、1 つのデバイスのドロップ率が 90 % であり、もう 1 つのデバイスのドロップ率が 10 % であることを示している可能性があります。また、両方のデバイスのドロップ率が 50 % である可能性もあります。グラフは、1 つのデバイスを選択した場合にのみ合計ドロップ率を表します。	No
データ ストリップが適用された RST パケットの正規化	[RST に関するデータを削除(Remove Data on RST)] を有効にします。	TCP リセット(RST)パケットからデータが削除されたパケットの数。	Yes
データ ストリップが適用された SYN パケットの正規化	[SYN に関するデータを削除(Remove Data on SYN)] を有効にします。	TCP オペレーティング システムが Mac OS でない場合に、SYN パケットからデータが削除されたパケットの数。	Yes
TCP ヘッダー パディングの正規化	[オプション パディング バイトの正規化またはクリア(Normalize/Clear Option Padding Bytes)] を有効にします。	オプションのパディング バイトが 0 に設定された TCP パケットの数。	Yes
TCP オプションなしの正規化	[これらの TCP オプションを許可(Allow These TCP Options)] を有効にして、[任意(any)] 以外のオプションに設定します。	タイムスタンプ オプションがストリップされたパケットの数。	Yes

表 41-1　侵入イベントのパフォーマンス グラフの種類(続き)

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
TCP NS フラグの正規化	[明示的輻輳通知(Explicit Congestion Notification)] を有効にして、[パケット(Packet)] を選択します。	ECN Nonce Sum(NS)オプション正規化の数。	Yes
TCP オプションの正規化	[これらの TCP オプションを許可(Allow These TCP Options)] を有効にして、[任意(any)] 以外のオプションに設定します。	オプション フィールドが No Operation(TCP オプション 1)に設定されているオプションの数(MSS、ウィンドウ スケール、タイムスタンプ、および明示的に許可されたオプションを除く)。	Yes
正規化によってブロックされた TCP パケット	[TCP ペイロードの正規化(Normalize TCP Payload)] を有効にします(セグメントのリアセンブリは失敗します)。	TCP セグメントを正常にリアセンブルできなかったためにドロップされたパケットの数。	Yes
TCP 予約済みフラグの正規化	[予約済みビットの正規化またはクリア(Normalize/Clear Reserved Bits)] を有効にします。	予約済みビットがクリアされた TCP パケットの数。	Yes
TCP セグメント リアセンブルの正規化	[TCP ペイロードの正規化(Normalize TCP Payload)] を有効にします(セグメントのリアセンブリは成功します)。	再送信データの一貫性を確保するために TCP データフィールドが正規化されたパケットの数(正しくリアセンブルできないセグメントはすべてドロップされます)。	Yes
TCP SYN オプションの正規化	[これらの TCP オプションを許可(Allow These TCP Options)] を有効にして、[任意(any)] 以外のオプションに設定します。	SYN 制御ビットが設定されていないため、最大セグメント サイズまたはウィンドウ スケール オプションが No Operation(TCP オプション 1)に設定されたオプションの数。	Yes
TCP タイムスタンプ ECR の正規化	[これらの TCP オプションを許可(Allow These TCP Options)] を有効にして、[任意(any)] 以外のオプションに設定します。	確認応答(ACK)制御ビットが設定されていないために、タイムスタンプ エコー応答(TSecr)オプション フィールドがクリアされたパケットの数。	Yes
TCP 緊急ポインタの正規化	[緊急ポインタの正規化(Normalize Urgent Pointer)] を有効にします。	TCP ヘッダーの緊急ポインタ フィールド(2 バイト)がペイロード長を超えていたために、ペイロード長に合わせてセットされたパケットの数。	Yes
ブロックされたパケットの総数	[インライン モード(Inline Mode)] または [インライン時にドロップ(Drop when Inline)] を設定します。	ルール、デコーダ、およびプリプロセッサのドロップを含む、ドロップされたパケットの総数。	No
インジェクトされたパケットの総数	[インライン モード(Inline Mode)] を設定します。	再送信前にサイズ変更されたパケットの数。	No

表 41-1　侵入イベントのパフォーマンス グラフの種類(続き)

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
TCP フィルタ適用パケットの総数	TCP ストリームの前処理を設定します。	TCP ポート フィルタリングのためにストリームによってスキップされたパケットの数。	No
UDP フィルタ適用パケットの総数	UDP ストリームの前処理を設定します。	UDP ポート フィルタリングのためにストリームによってスキップされたパケットの数。	No
緊急フラグ クリア済みの正規化	[緊急ポインタが設定されていない場合 URG をクリア(Clear URG if Urgent Pointer is Not Set)] を有効にします。	緊急ポインタが設定されていなかったために、TCP ヘッダーの URG 制御ビットがクリアされたパケットの数。	Yes
緊急ポインタおよび緊急フラグ クリア済みの正規化	[空のペイロードに設定された緊急ポインタまたは URG をクリア(Clear Urgent Pointer/URG on Empty Payload)] を有効にします。	ペイロードがなかったために、TCP ヘッダーの緊急ポインタ フィールドと URG 制御ビットがクリアされたパケットの数。	Yes
緊急ポインタ クリア済みの正規化	[URG=0 の場合に緊急ポインタをクリア(Clear Urgent Pointer if URG=0)] を有効にします。	緊急(UGR)制御ビットが設定されていなかったために、TCP ヘッダーの緊急ポインタ フィールド(16 ビット)がクリアされたパケットの数。	Yes

侵入イベントのパフォーマンス グラフを生成する方法:

アクセス: Admin/Maint

手順 1　[概要(Overview)] > [概要(Summary)] > [侵入イベント パフォーマンス(Intrusion Event Performance)] を選択します。

[侵入イベント パフォーマンス(Intrusion Event Performance)] ページが表示されます。

手順 2　[デバイスの選択(Select Device)] リストから、データを表示するデバイスを選択します。

手順 3　[グラフの選択(Select Graph(s))] リストから、作成するグラフの種類を選択します。

手順 4　[時間帯の選択(Select Time Range)] リストから、グラフに使用する時間範囲を選択します。

過去 1 時間、前日、先週、または先月から選択できます。

手順 5　[グラフ(Graph)] をクリックします。

グラフが表示され、ユーザが指定した情報が表示されます。

手順 6　グラフを保存するには、グラフを右クリックし、ブラウザでイメージを保存する手順に従います。

侵入イベント グラフの表示

ライセンス：Protection

FireSIGHT システムは、経時的な侵入イベントの傾向を示すグラフを表示します。以下に関する侵入イベントについて、過去 1 時間から先月までの範囲の経時的なグラフを生成できます。

- 1 つまたはすべての管理対象デバイス
- 上位 10 個の宛先ポート
- 上位 10 個の送信元 IP アドレス
- 上位 10 個のイベント メッセージ

イベント グラフを生成する方法：

アクセス：Admin/Intrusion Admin

手順 1　[概要（Overview）] > [概要（Summary）] > [侵入イベント グラフ（Intrusion Event Graphs）] を選択します。

[侵入イベント グラフ（Intrusion Event Graphs）] ページが表示されます。ページの上部にある 3 つの選択ボックスは、どのグラフを生成するかを制御します。

手順 2　[デバイスの選択（Select Device）] で、[すべて（all）] を選択してすべてのデバイスを含めるか、グラフに含める特定のデバイスを選択します。

手順 3　[グラフの選択（Select Graph(s)）] で、生成するグラフの種類を選択します。

手順 4　[時間範囲を選択してください（Select Time Range）] で、グラフの時間範囲を選択します。

手順 5　[グラフ（Graph）] をクリックします。

グラフが生成されます。

侵入イベントの表示

ライセンス：Protection

システムは、悪意のある可能性があるパケットを認識すると、侵入イベントを生成し、イベントをデータベースに追加します。

初期の侵入イベント ビューは、ページにアクセスするために使用するワークフローによって異なります。1 つ以上のドリルダウン ページ、侵入イベントのテーブル ビュー、および終了パケット ビューを含む、定義済みワークフローの 1 つを使用するか、独自のワークフローを作成できます。カスタム テーブルに基づいてワークフローを表示することもできます。これには、侵入イベントを含めることができます。大量の IP アドレスが含まれている状態で、[IP アドレスの解決（Resolve IP Addresses）] イベント ビュー設定が有効になっている場合、イベント ビューの表示が遅くなる場合があることに注意してください。詳細については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

侵入イベントは、ネットワーク セキュリティに対する脅威があるかどうかを判断するために表示します。侵入イベントが悪意のあるものではないことがわかったら、そのイベントを確認済みとしてマークできます。ユーザの名前がレビューアとして表示され、確認されたイベントはデフォルトの侵入イベント ビューには表示されなくなります。イベントに未確認のマークを付けることによって、確認済みイベントをデフォルトの侵入イベント ビューに戻すことができます。

確認済みとしてマークした侵入イベントを表示できます。確認済みのイベントはイベント データベースに保存され、イベント要約統計に含まれますが、デフォルトのイベント ページには表示されなくなります。詳細については、侵入イベントの確認（41-18 ページ）を参照してください。

バックアップを実行してから確認済みの侵入イベントビューを削除した場合、バックアップを復元すると、削除された侵入イベント ビューは復元されますが、確認済みのステータスは復元されません。復元されたそれらの侵入イベントは、[確認済みイベント（Reviewed Events）] の下ではなく [侵入イベント（Intrusion Events）] の下に表示されます。

1 つ以上の侵入イベントと関連付けられた接続イベントを素早く表示するには、イベント ビューアのチェックボックスを使用して侵入イベントを選択してから、[移動先（Jump to）] ドロップダウン リストから [接続（Connections）] を選択します。これは、イベントのテーブル ビュー間を移動する場合に非常に役立ちます。同じ方法で、特定の接続に関連した侵入を表示することもできます。

詳細については、次の項を参照してください。

- 侵入イベントについて（41-12 ページ）
- カスタム ワークフローの作成（58-44 ページ）
- ドリルダウン ページとテーブル ビュー ページの使用（41-21 ページ）
- パケット ビューの使用（41-25 ページ）
- 侵入イベントと関連付けられた接続データの表示（41-17 ページ）
- 侵入イベントの確認（41-18 ページ）
- カスタム テーブルに基づいたワークフローの表示（59-10 ページ）

侵入イベントを表示する方法:

アクセス: Admin/Intrusion Admin

手順 1　[分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）] を選択します。

デフォルトの侵入イベントのワークフローの最初のページが表示されます。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されない場合は、時間範囲の調整が必要な可能性があります。イベント時間の制約の設定（58-27 ページ）を参照してください。

ヒント　侵入イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合、ワークフローのタイトルの横にある [（ワークフローの切り替え）（(switch workflow)）] をクリックして、アプライアンスに付属の定義済みワークフローのいずれかを選択します。

侵入イベント ビューに表示されるイベントの詳細については、侵入イベントについて（41-12 ページ）を参照してください。分析にとって重要な侵入イベントにビューを絞り込む方法の詳細については、侵入イベントのワークフロー ページについて（41-20 ページ）を参照してください。

侵入イベントについて

ライセンス：Protection

システムは、ネットワークを通過するパケットを検査し、ホストとそのデータの可用性、整合性、および機密性に影響を与える可能性がある悪意のあるアクティビティについて調べます。システムは、潜在的な侵入を特定すると*侵入イベント*を生成します。これは、エクスプロイトの日付、時間、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報の記録です。パケットベースのイベントの場合、イベントをトリガーしたパケットのコピーも記録されます。個々の侵入イベントで利用可能な情報は、ライセンスなどいくつかの要因に応じて決まります。詳細については、サービス サブスクリプション（65-8 ページ）を参照してください。

次のリストで、侵入イベントに含まれる情報について説明します。侵入イベントのテーブルビューの一部のフィールドはデフォルトで無効になっていることに注意してください。セッション中にフィールドを有効にするには、展開矢印（）をクリックして、検索制約を拡張してから、[無効列（Disabled Columns）] の下の列名をクリックします。

時刻（Time）

イベントの日時。

[プライオリティ（Priority）]

シスコ VRT で指定されたイベントの優先度。

影響（Impact）

このフィールドの影響レベルは、侵入データ、ネットワーク検出データ、脆弱性情報との関係を示します。詳細については、影響レベルを使用してイベントを評価する（41-41 ページ）を参照してください。

NetFlow データに基づいてネットワーク マップに追加されたホストで使用可能なオペレーティング システム情報が存在しない場合、ホスト入力機能を使用してホストオペレーティングシステムのアイデンティティを手動で設定しない限り、防御センター はこれらのホストに関係した侵入イベントに対して影響レベル [脆弱（Vulnerable）]（影響レベル 1：赤）を割り当てることができないことに注意してください。

インライン結果（Inline Result）

次のいずれかです。

- 黒い下矢印。ルールをトリガーとして使用したパケットをシステムがドロップしたことを示します
- 灰色の下矢印：[インライン時にドロップ（Drop when Inline）] 侵入ポリシー オプション（インライン展開環境）を有効にした場合、またはシステムがプルーニングしている間に [ドロップしてイベントを生成する（Drop and Generate）] ルールがイベントを生成した場合、IPS がパケットをドロップしたことを示します
- ブランク。トリガーとして使用されたルールが [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていないことを示します

  侵入ポリシーのルールの状態またはインライン ドロップ動作にかかわらず、インライン インターフェイスがタップ モードになっている場合を含め、パッシブ展開環境ではシステムはパケットをドロップしないことに注意してください。

ソース IP

送信元ホストが使用する IP アドレス。

送信元の国（Source Country）

送信元ホストの国。

宛先 IP（Destination IP）

受信ホストが使用する IP アドレス。

宛先の国（Destination Country）

受信ホストの国。

元のクライアント IP（Original Client IP）

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーから取得された、元のクライアント IP アドレス。このフィールドの値を表示するには、ネットワーク分析ポリシーの HTTP プリプロセッサの [クライアントのオリジナル IP アドレスの抽出（Extract Original Client IP Address）] オプションを有効にする必要があります。オプションで、ネットワーク分析ポリシーの同じエリアで、最大 6 つのカスタム クライアント IP ヘッダーを指定し、システムによって [元のクライアント IP（Original Client IP）] イベント フィールドの値が選択される優先順位を設定します。詳細については、サーバレベル HTTP 正規化オプションの選択（27-36 ページ）を参照してください。

このフィールドは、デフォルトで有効になっています。

送信元ポート/ICMP タイプ（Source Port / ICMP Type）

送信元ホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP タイプを表示します。

宛先ポート/ICMP コード（Destination Port / ICMP Code）

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP コードを表示します。

SSL ステータス（SSL Status）

SSL ルールに関連したアクション、デフォルトのアクション、または暗号化接続をログに記録した復号できないトラフィック アクション。

- [ブロック（Block）] および [リセットしてブロック（Block with reset）] は、ブロックされた暗号化接続を表します。
- [復号（再署名）（Decrypt (Resign)）] は、再署名サーバ証明書を使用して復号された発信接続を表します。
- [復号（キーの置き換え）（Decrypt (Replace Key)）] は、置き換えられた公開キーと自己署名サーバ証明書を使用して復号された発信接続を表します。
- [復号（既知のキー）（Decrypt (Known Key)）] は、既知の秘密キーを使用して復号された着信接続を表します。
- [復号しない（Do not Decrypt）] は、システムが復号しなかった接続を表します。

システムが暗号化接続を復号できなかった場合は、実行された復号不能のトラフィック アクションと障害の理由が表示されます。たとえば、システムが不明な暗号スイートで暗号化されたトラフィックを検出し、さらにインスペクションを行わずにそのトラフィックを許可した場合、このフィールドには `[復号しない（不明な暗号スイート）（Do Not Decrypt （Unknown Cipher Suite））]` が表示されます。

証明書の詳細を表示するにはロック アイコン（  ）をクリックします。詳細については、暗号化接続に関連付けられた証明書の表示（39-34 ページ）を参照してください。

VLAN ID（Admin. VLAN ID）

侵入イベントをトリガーしたパケットに関連付けられている最内部 VLAN ID。

MPLS ラベル（MPLS Label）

この侵入イベントをトリガーしたパケットと関連付けられているマルチプロトコル ラベル スイッチング ラベル。

このフィールドは、デフォルトでは無効です。

メッセージ（Message）

イベントを説明するテキスト。ルールベースの侵入イベントの場合、イベント メッセージはルールから取得されます。デコーダベースおよびプリプロセッサベースのイベントの場合は、イベント メッセージはハード コーディングされています。

分類（Classification）

イベントを生成したルールが属する分類。ルールの分類名と番号のリストについては、ルールの分類の表を参照してください。

ジェネレータ（Generator）

イベントを生成したコンポーネント。侵入イベント ジェネレータ ID のリストについては、表 41-7（41-44 ページ）を参照してください。

送信元ユーザ（Source User）

送信元ホストにログインしている既知のユーザのユーザ ID。

宛先ユーザ（Destination User）

宛先ホストにログインしている既知のユーザのユーザ ID。

アプリケーション プロトコル（Application Protocol）

（使用可能な場合）侵入イベントをトリガーしたトラフィックで検出されたホスト間の通信を表す、アプリケーション プロトコル。防御センター Web インターフェイスで検出されたアプリケーション プロトコルをシステムが特定するしくみについては、表 45-3（45-14 ページ）を参照してください。

クライアント（Client）

（使用可能な場合）侵入イベントをトリガーしたトラフィックで検出されたモニタ対象のホストで実行されているソフトウェアを表す、クライアント アプリケーション。

Web アプリケーション（Web Application）

侵入イベントをトリガーしたトラフィックで検出された HTTP トラフィックの内容または要求された URL を表す、Web アプリケーション。

システムが HTTP のアプリケーション プロトコルを検出したものの、特定の Web アプリケーションを検出できない場合は、一般的な Web ブラウジングの指定がここで提示されるので注意してください。

IOC

侵入イベントをトリガーしたトラフィックが、接続に関係するホストに対する侵入の兆候（IOC）もトリガーしたかどうか。IOC の詳細については、侵害の兆候（痕跡）について（45-22 ページ）を参照してください。

大項目、タグ（アプリケーション プロトコル、クライアント、Web アプリケーション）（Category, Tag (Application Protocol, Client, Web Application)）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準（表 45-2（45-12 ページ）を参照）。

アプリケーションのリスク（Application Risk）

侵入イベントをトリガーしたトラフィックで検出されたアプリケーションに関連付けられたリスク。接続で検出されるアプリケーションのタイプごとに関連するリスクがあります。このフィールドは、それらのうち最も高いリスクを表示します。詳細については、表 45-2（45-12 ページ）を参照してください。

ビジネスとの関連性（Business Relevance）

侵入イベントをトリガーしたトラフィックで検出されたアプリケーションに関連付けられた、ビジネスとの関連性。接続で検出されるアプリケーションのタイプごとに関連するビジネスとの関連性があります。このフィールドは、それらのうち最も低い（関連性が最も低い）ものを表示します。詳細については、表 45-2（45-12 ページ）を参照してください。

入力セキュリティ ゾーン（Ingress Security Zone）

イベントをトリガーしたパケットの入力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。セキュリティ ゾーンの操作（3-44 ページ）を参照してください。

出力セキュリティ ゾーン（Egress Security Zone）

インライン展開環境の場合、イベントをトリガーしたパケットの出力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーンのフィールドには入力されません。セキュリティ ゾーンの操作（3-44 ページ）を参照してください。

Device

アクセス コントロール ポリシーが適用された管理対象デバイス。デバイスの管理（4-1 ページ）を参照してください。

セキュリティ コンテキスト（Security Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチ コンテキスト モードの ASA FirePOWER デバイスだけです。

入力インターフェイス（Ingress Interface）

イベントをトリガーしたパケットの入力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列だけに入力されます。センシング インターフェイスの設定（4-66 ページ）を参照してください。

出力インターフェイス（Egress Interface）

インライン セットの場合、イベントをトリガーしたパケットの出力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列には入力されません。センシング インターフェイスの設定（4-66 ページ）を参照してください。

侵入ポリシー（Intrusion Policy）

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。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）および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）を参照してください。

アクセス コントロール ポリシー（Access Control Policy）

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効になっている侵入ポリシーを含んでいるアクセス コントロール ポリシー（アクセス コントロール ポリシーの管理（12-12 ページ）を参照）。

アクセス コントロール ルール（Access Control Rule）

イベントを生成した侵入ポリシーを呼び出したアクセス コントロール ルール（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）を参照）。[デフォルト アクション（Default Action）] は、ルールが有効化されている侵入ポリシーが特定のアクセス コントロール ルールに関連付けられておらず、代わりに、アクセス コントロール ポリシーのデフォルト アクションとして設定されていることを示しています（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）を参照）。

侵入インスペクションがアクセス コントロール ルールにもデフォルト アクションにも関連付けられていない場合、このフィールドは空欄になります。たとえば、パケットがデフォルトの侵入ポリシーによって検査された場合などです。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。

ネットワーク分析ポリシー（Network Analysis Policy）

（存在する場合）イベントの生成に関連付けられているネットワーク分析ポリシー（NAP）（ネットワーク分析ポリシーの準備（26-1 ページ）を参照）。

HTTP ホスト名（HTTP Hostname）

HTTP 要求のホスト ヘッダーから取得されたホスト名（存在する場合）。要求パケットにホスト名が常に含まれているわけではないことに注意してください。

ホスト名を表示するには、HTTP 検査プリプロセッサの [ホスト名の記録（Log Hostname）] オプションを有効にする必要があります。詳細については、サーバレベル HTTP 正規化オプションの選択（27-36 ページ）を参照してください。

この列には、取得されたホスト名の最初の 50 文字が表示されます。ホストの省略名の表示部分にポインタを合わせると、最大 256 バイトまでの完全な名前を表示することができます。また、最大 256 バイトまでの完全なホスト名をパケット ビューに表示することもできます。詳細については、イベント情報の表示（41-27 ページ）を参照してください。

このフィールドは、デフォルトでは無効です。

HTTP URI

（存在する場合）侵入イベントをトリガーした HTTP 要求パケットに関連付けられた raw URI。要求パケットに URI が常に含まれているわけではないことに注意してください。

取得された URI を表示するには、HTTP 検査プリプロセッサの [URI の記録（Log URI）] オプションを有効にする必要があります。詳細については、サーバレベル HTTP 正規化オプションの選択（27-36 ページ）を参照してください。

HTTP 応答によってトリガーされた侵入イベントの関連 HTTP URI を参照するには、[両ポートでのストリーム リアセンブルの実行（Perform Stream Reassembly on Both Ports）] オプションに HTTP サーバのポートを設定する必要があります。ただし、これにより、トラフィックのリアセンブル用のリソース要求が増加することに注意してください。ストリーム再構成のオプションの選択（29-30 ページ）を参照してください。

この列には、取得された URI の最初の 50 文字が表示されます。省略 URI の表示部分にポインタを合わせると、最大 2048 バイトまでの完全な URI を表示することができます。また、最大 2048 バイトまでの完全な URI をパケット ビューに表示することもできます。詳細については、イベント情報の表示（41-27 ページ）を参照してください。

このフィールドは、デフォルトでは無効です。

メール送信者（Email Sender）

SMTP MAIL FROM コマンドから取得された電子メール送信者のアドレス。このフィールドの値を表示するには、SMTP プリプロセッサの [送信者アドレスのログ（Log From Address）] オプションを有効にする必要があります。複数の送信者アドレスがサポートされます。詳細については、SMTP デコードについて（27-65 ページ）を参照してください。

このフィールドは、デフォルトでは無効です。

電子メール受信者（Email Recipient）

SMTP RCPT TO コマンドから取得された電子メール受信者のアドレス。このフィールドの値を表示するには、SMTP プリプロセッサの [受信者アドレスのログ（Log To Addresses）] オプションを有効にする必要があります。複数の受信者アドレスがサポートされます。詳細については、SMTP デコードについて（27-65 ページ）を参照してください。

このフィールドは、デフォルトでは無効です。

電子メール添付ファイル（Email Attachments）

MIME Content-Disposition ヘッダーから取得された MIME 添付ファイル名。添付ファイルの名前を表示するには、SMTP プリプロセッサの [MIME 添付ファイル名の記録（Log MIME Attachment Names）] オプションを有効にする必要があります。複数の添付ファイル名がサポートされます。詳細については、SMTP デコードについて（27-65 ページ）を参照してください。

このフィールドは、デフォルトでは無効です。

確認者（Reviewed By）

イベントを確認したユーザの名前。侵入イベントの確認（41-18 ページ）を参照してください。

メンバー数（Count）

各行に表示された情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

侵入イベントと関連付けられた接続データの表示

ライセンス：Protection

システムは、侵入イベントが検出された接続を記録できます。このロギングは、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に対して自動的に行われますが、デフォルト アクションに関連する接続データを参照するには、接続ロギングを手動で有効にする必要があります（アクセス コントロールの処理に基づく接続のロギング（38-18 ページ）を参照）。

（注）　個々の接続またはセキュリティ インテリジェンス イベントで利用可能な情報は、ライセンスやアプライアンス モデルなど、いくつかの要因によって異なります。詳細については、接続ロギングのライセンスおよびモデル要件（38-11 ページ）を参照してください。

1 つ以上の侵入イベントに関連付けられた接続データを表示する方法：

アクセス：管理

手順 1　[分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）] を選択します。

デフォルトの侵入イベントのワークフローの最初のページが表示されます。

関連データの表示は、イベントのテーブル ビュー間を移動する場合に非常に役立ちます。分析にとって重要な侵入イベントにビューを絞り込む方法の詳細については、侵入イベントのワークフロー ページについて（41-20 ページ）を参照してください。

手順 2　イベント ビューアのチェックボックスを使用して侵入イベントを選択してから、[移動先（Jump to）] ドロップダウン リストから [接続（Connections）] を選択します。

同じ方法で、特定の接続に関連した侵入イベントを表示できます。詳細については、ワークフロー間のナビゲート（58-41 ページ）を参照してください。

関連イベントを確認するとき、防御センター はデフォルトの接続データのワークフローを使用します。接続データの詳細については、接続およびセキュリティ インテリジェンスのデータの使用（39-1 ページ）を参照してください。

ヒント　侵入イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合、ワークフローのタイトルの横にある [（ワークフローの切り替え）（(switch workflow)）] をクリックして、アプライアンスに付属の定義済みワークフローのいずれかを選択します。

侵入イベントの確認

ライセンス：Protection

侵入イベントを調べて、そのイベントがネットワーク セキュリティに対して脅威ではないことがわかったら（おそらく、ネットワーク上のどのホストも検出されたエクスプロイトに対して脆弱でないことがわかったため）、そのイベントを確認済みとしてマークできます。ユーザの名前がレビューアとして表示され、確認されたイベントはデフォルトの侵入イベント ビューには表示されなくなります。確認済みとしてマークしたイベントはイベント データベースに残りますが、侵入イベントのビューには表示されなくなります。

侵入イベントに確認済みのマークを付けるには：

アクセス：Admin/Intrusion Admin

手順 1　侵入イベントが表示されるページで、次の 2 つの方法を選択できます。

- イベントのリストから 1 つまたは複数の侵入イベントにマークを付けるには、イベントの横にあるチェックボックスを選択し、[確認（Review）] をクリックします。
- イベントのリストからすべての侵入イベントにマークを付けるには、[すべて確認（Review All）] をクリックします。

成功メッセージが表示され、確認済みイベント リストが更新されます。

侵入イベント ビューに表示されるイベントの詳細については、侵入イベントについて（41-12 ページ）を参照してください。分析にとって重要な侵入イベントにビューを絞り込む方法の詳細については、侵入イベントのワークフロー ページについて（41-20 ページ）を参照してください。

（注）　確認されたイベントは、侵入イベントに関連したワークフローのページに表示されませんが、イベント要約の統計情報には含まれます。

以前に確認済みとマークされたイベントを表示する方法:

アクセス: Admin/Intrusion Admin

手順 1　[分析（Analysis）] > [侵入（Intrusions）] > [確認済みイベント（Reviewed Events）] を選択します。

デフォルトの確認済み侵入イベントのワークフローの最初のページが表示されます。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されない場合は、時間範囲の調整が必要な可能性があります。イベント時間の制約の設定（58-27 ページ）を参照してください。

ヒント　侵入イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合、ワークフローのタイトルの横にある [（ワークフローの切り替え）（(switch workflow)）] をクリックして、アプライアンスに付属の定義済みワークフローのいずれかを選択します。

確認済み侵入イベント ビューに表示されるイベントの詳細については、侵入イベントについて（41-12 ページ）を参照してください。分析にとって重要な侵入イベントにビューを絞り込む方法の詳細については、侵入イベントのワークフロー ページについて（41-20 ページ）を参照してください。

確認済みイベントに未確認のマークを付けるには:

アクセス: Admin/Intrusion Admin

手順 1　確認済みイベントが表示されるページで、次の 2 つの方法を選択できます。

- 確認済みイベント リストから個別の侵入イベントを削除するには、イベントの横にあるチェックボックスを選択し、[未確認（Unreview）] をクリックします。
- 確認済みイベント リストからすべての侵入イベントを削除するには、[すべて未確認（Unreview All）] をクリックします。

成功メッセージが表示され、確認済みイベント リストが更新されます。

侵入イベントのワークフロー ページについて

ライセンス：Protection

現在の侵入ポリシーで有効になっているプリプロセッサ、デコーダ、および侵入ルールは、モニタしているトラフィックがポリシーに違反するたびに、侵入イベントを生成します。

FireSIGHT システムは、侵入イベントの表示および分析に使用できる、イベント データが入力された定義済みワークフローのセットを提供します。これらのワークフローは、評価する侵入イベントの特定に役立つ一連のページを表示して手順を示します。

定義済みの侵入イベントのワークフローには、次の 3 種類のページまたはイベント ビューがあります。

- 1 つ以上のドリルダウン ページ
- 侵入イベントのテーブル ビュー
- パケット ビュー

*ドリルダウン ページ*には通常、1 つの特定の種類の情報を表示できるように、1 つのテーブル（一部のドリルダウン ビューでは複数のテーブル）に複数の列が含まれています。

「ドリルダウン」して 1 つ以上の宛先ポートの詳細情報を検索すると、これらのイベントは自動的に選択され、ワークフローの次のページが表示されます。このように、ドリルダウン テーブルを使用すると、一度に分析するイベントの数を削減できます。

侵入イベントの最初の *テーブル ビュー*では、各侵入イベントが独自の行にリストされます。テーブルの列には、時間、送信元 IP アドレスおよびポート、宛先 IP アドレスおよびポート、イベントの優先順位、イベント メッセージなどの情報が示されます。

イベントを選択してワークフローの次のページを表示する代わりに、テーブル ビューでイベントを選択した場合、イベントはいわゆる *制約*に追加されます。制約とは、分析するイベントの種類に加える制限のことです。

たとえば、任意の列で列のクローズ アイコン（ ）をクリックして、ドロップダウン リストから [時間（Time）] をクリアすると、[時間（Time）] を列の 1 つとして削除できます。分析内でイベントのリストを絞り込むには、テーブル ビューの行のいずれかの値のリンクをクリックします。たとえば、分析を送信元 IP アドレスの 1 つ（おそらく、潜在的な攻撃者）から生成されたイベントに制限するには、[送信元 IP アドレス（Source IP Address）] 列の IP アドレスをクリックします。

テーブル ビューの 1 つまたは複数の行を選択し、[表示（View）] をクリックすると、パケット ビューが表示されます。*パケット ビュー*は、ルールをトリガーしたパケットまたはイベントを生成したプリプロセッサに関する情報を提供します。パケット ビューの各セクションには、パケット内の特定の層についての情報が含まれます。折りたたまれたセクションを展開すると、より多くの情報を参照できます。

（注） それぞれのポートスキャン イベントは複数のパケットによってトリガーされるため、ポートスキャン イベントは特別なバージョンのパケット ビューを使用します。詳細については、ポートスキャンの検出（34-3 ページ）を参照してください。

事前定義済みのワークフローが特定のニーズに合致しない場合は、必要な情報だけを表示するカスタム ワークフローを作成できます。カスタム侵入イベントのワークフローには、ドリルダウン ページ、イベントのテーブル ビュー、またはその両方を含めることができます。システムはパケット ビューを最後のページとして自動的に組み込みます。イベントを調査する方法に応じて、定義済みワークフローと独自のカスタム ワークフローを簡単に切り替えることができます。

ヒント　ワークフローの概要と使用（58-1 ページ）は、すべてのワークフロー ページに共通のワークフローおよび機能の使用方法について説明します。この章では、カスタム侵入イベントのワークフローを作成および使用する方法についても説明します。

詳細については、以下を参照してください。

- ドリルダウン ページとテーブル ビュー ページの使用（41-21 ページ）には、多くの共通機能を共有している、ドリルダウン ページとイベントのテーブル ビューの使用方法が記載されています。
- パケット ビューの使用（41-25 ページ）では、パケット ビューで機能を使用する方法について説明します。
- 侵入イベントの検索（41-46 ページ）では、イベント データベースで特定の侵入イベントを検索する方法について説明します。

ドリルダウン ページとテーブル ビュー ページの使用

ライセンス：Protection

侵入イベントを調査するために使用できるワークフローでは、次の 3 種類のページが利用されます。

- ドリルダウン ページ
- 侵入イベントのテーブル ビュー
- パケット ビュー

これらの各ページについては、侵入イベントのワークフロー ページについて（41-20 ページ）で説明されています。

イベントのドリルダウン ビューとテーブル ビューはいくつかの共通機能を共有しています。これらの機能を使用して、イベントのリストを絞り込み、関連するイベントのグループを集中的に分析できます。次の表に、これらの機能について説明します。

表 41-2　侵入イベントの共通機能

目的	操作
表示された列の詳細を表示する	侵入イベントについて（41-12 ページ）で詳細を参照してください。
ホストのプロファイルを表示する	ホスト IP アドレスの横に表示されるホスト プロファイル アイコン（  ）をクリックします。
地理位置情報の詳細の表示	[送信元の国（Source Country）] または [宛先の国（Destination Country）] 列に表示されるフラグ アイコンをクリックします。
表示されたイベントの時刻と日付の範囲を変更する	イベント時間の制約の設定（58-27 ページ）で詳細を参照してください。 イベント ビューを時間によって制約している場合は、（グローバルかイベント固有かに関係なく）アプライアンスに設定されている時間枠の外で生成されたイベントが、イベント ビューに表示されることがあるので注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

表 41-2　侵入イベントの共通機能（続き）

目的	操作
現在のワークフロー ページでイベントをソートしたり、制限したりする	詳細については、以下を参照してください。 • ドリルダウン ワークフロー ページのソート（58-39 ページ） • ドリルダウン ページでのイベントの制約表 • イベントのテーブル ビューのイベントの制約表
現在のワークフロー ページ内で移動する	ワークフロー内の他のページへのナビゲート（58-40 ページ）で詳細を参照してください。 **ヒント**　別のワークフロー ページで同じ侵入イベントを表示しないようにするため、ページの下部にあるリンクをクリックして別のページのイベントを表示すると時間範囲は一時停止し、クリックして後続のページでその他のアクションを実行すると再開します。詳細については、イベント時間の制約の設定（58-27 ページ）を参照してください。
現在の制限を維持して、現在のワークフロー内のページ間を移動する	ワークフロー ページの左上で、該当するページ リンクをクリックします。詳細については、ワークフローのページの使用（58-21 ページ）を参照してください。
後でインシデントに転送できるようにイベントをクリップボードに追加する	次のいずれかの方法を使用します。 • ワークフロー ページの複数の侵入イベントをクリップボードにコピーするには、コピーするイベントの横にあるチェックボックスを選択して、[コピー（Copy）] をクリックします。 • 現在制約されているビューにあるすべての侵入イベントをクリップボードにコピーするには、[すべてをコピー（Copy All）] をクリックします。 クリップボードはユーザごとに最大 25,000 個のイベントを保存します。詳細については、クリップボードの使用（41-54 ページ）を参照してください。
イベント データベースからのイベントの削除	次のいずれかの方法を使用します。 • 選択した侵入イベントを削除するには、削除するイベントの横にあるチェックボックスを選択し、[削除（Delete）] をクリックします。 • 現在制約されているビューにあるすべての侵入イベントを削除するには、[すべて削除（Delete All）] をクリックし、すべてのイベントを削除してよいかどうかを確認します。
イベントに確認済みのマークを付けて、侵入イベントのページからそれらを削除し、イベント データベースからは削除しない	次のいずれかの方法を使用します。 • 選択した侵入イベントを確認するには、確認するイベントの横にあるチェックボックスを選択し、[確認（Review）] をクリックします。 • 現在制約されているビューにあるすべての侵入イベントを確認するには、[すべて確認（Review All）] をクリックします。 詳細については、侵入イベントの確認（41-18 ページ）を参照してください。

表 41-2　侵入イベントの共通機能（続き）

目的	操作
選択した各イベントをトリガーしたパケット（libpcap 形式のパケット キャプチャ ファイル）のローカル コピーをダウンロードする	次のいずれかの方法を使用します。 • 選択した侵入イベントをトリガーしたパケットをダウンロードするには、ダウンロードするパケットによってトリガーされたイベントの横にあるチェックボックスを選択し、[パケットのダウンロード（Download Packets）] をクリックします。 • 現在制約されているビューにある侵入イベントをトリガーしたすべてのパケットをダウンロードするには、[すべてのパケットのダウンロード（Download All Packets）] をクリックします。 キャプチャされたパケットは libpcap 形式で保存されます。この形式は、複数の一般的なプロトコル アナライザで使用されます。
他のイベント ビューに移動して関連イベントを表示する	ワークフロー間のナビゲート（58-41 ページ）で詳細を参照してください。
一時的に他のワークフローを使用する	[（ワークフローの切り替え）（(switch workflow)）] をクリックします。詳細については、ワークフローの選択（58-19 ページ）を参照してください。
すぐに再表示できるように、現在のページをブックマークする	[このページをブックマーク（Bookmark This Page）] をクリックします。詳細については、ブックマークの使用（58-42 ページ）を参照してください。
[概要ダッシュボード（Summary Dashboard）] の [侵入イベント（Intrusion Events）] セクションを表示する	[ダッシュボード（Dashboards）] をクリックします。詳細については、ダッシュボードの操作（55-42 ページ）を参照してください。
ブックマークの管理ページへ移動する	[ブックマークの表示（View Bookmarks）] をクリックします。詳細については、ブックマークの使用（58-42 ページ）を参照してください。
現在のビューのデータに基づいてレポートを生成する	[レポート デザイナ（Report Designer）] をクリックします。詳細については、イベント ビューからのレポート テンプレートの作成（57-10 ページ）を参照してください。

イベント ビューに表示される侵入イベントの数は、次の内容によっては非常に多くなることがあります。

- ユーザが選択する時間範囲
- ネットワークのトラフィック量
- 適用する侵入ポリシー

侵入イベントをさらに分析しやすくするために、イベント ページを制約できます。制約プロセスは、侵入イベントのドリルダウン ビューとテーブル ビューとでは若干異なります。

ヒント　時間範囲は、侵入イベントのワークフロー ページの下部にあるリンクの 1 つをクリックして別のページに移動したときに一時停止し、クリックして後続のページでワークフローの終了を含む別のアクションを実行したときに再開します。これにより、ワークフロー内の他のページに移動してより多くのイベントを参照した場合に、同じイベントが表示される可能性が減ります。詳細については、イベント時間の制約の設定（58-27 ページ）およびワークフロー内の他のページへのナビゲート（58-40 ページ）を参照してください。

次の表では、ドリルダウン ページの使用方法を示しています。

表 41-3　ドリルダウン ページでのイベントの制約

目的	操作
次のワークフロー ページのドリルダウンを特定の値に制約する	値をクリックします。 たとえば、[宛先ポート（Destination Port）] ワークフローで、イベントを宛先ポートが 80 であるものに制約するには、[DST ポート/ICMP コード（DST Port/ICMP Code）] 列で [80/tcp（80/tcp）] をクリックします。ワークフローの次のページ [イベント（Events）] が表示され、ポート 80/tcp のイベントだけが含まれます。
次のワークフロー ページのドリルダウンを選択したイベントに制約する	次のワークフロー ページで表示するイベントの横にあるチェックボックスを選択し、[表示（View）] をクリックします。 たとえば、[宛先ポート（Destination Port）] ワークフローで、イベントを宛先がポート 20/tcp および 21/tcp であるものに制約するには、それらのポートの行の横にあるチェックボックスを選択し、[表示（View）] をクリックします。ワークフローの次のページ [イベント（Events）] が表示され、ポート 20/tcp および 21/tcp のイベントだけが含まれます。 **（注）** 複数の行を制約し、テーブルに複数の列が存在する場合（[カウント（Count）] 列を含まない）、いわゆる複合制約が作成されます。複合制約により、必要以上のイベントを制約に含めないようにすることができます。たとえば、[イベントと接続先（Event and Destination）] ワークフローを使用する場合は、最初のドリルダウン ページで選択した各行により、複合制約が作成されます。宛先 IP アドレス 10.10.10.100 のイベント 1:100 を選択し、宛先 IP アドレス 192.168.10.100 のイベント 1:200 も選択した場合、複合制約により、イベント タイプとして 1:100 を含むイベントや宛先 IP アドレスとして 192.168.10.100 を含むイベント、またはイベント タイプとして 1:200 を含むイベントや宛先 IP アドレスとして 10.10.10.100 を含むイベントが選択されないようになります。
現在の制約を保持しながら、次のワークフロー ページをドリルダウンする	[すべて表示（View All）] をクリックします。

次の表では、テーブル ビューの使用方法について説明します。

表 41-4　イベントのテーブル ビューのイベントの制約

目的	操作
1 つの属性を持つイベントにビューを制約する	属性をクリックします。 たとえば、宛先がポート 80 であるイベントにビューを制約するには、[DST ポート/ICMP コード（DST Port/ICMP Code）] 列で [80/tcp（80/tcp）] をクリックします。
テーブルから列を削除する	非表示にするカラムの見出しで、クローズ アイコン（ ）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。 **ヒント** 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、対象のチェック ボックスをオンまたはオフにします。無効になったカラムをビューに戻すには、展開アイコン（ ）をクリックして検索の制約を展開し、[無効になったカラム（Disabled Columns）] の下にあるカラム名をクリックします。

表 41-4　イベントのテーブル ビューのイベントの制約(続き)

目的	操作
1 つ以上のイベントに関連付けられたパケットを表示する	次のいずれかを行います。 • パケットを表示するイベントの横にある下矢印アイコン( )をクリックします。 • パケットを表示する 1 つ以上のイベントを選択し、ページの下部にある [表示(View)] をクリックします。 • ページの下部で、[すべて表示(View All)] をクリックして、現在の制約に一致するすべてのイベントのパケットを表示します。

ヒント　プロセスの任意の時点で、制約を検索条件のセットとして保存できます。たとえば、ネットワークが数日にわたり単一の IP アドレスから攻撃者によって探られていることに気付いた場合、調査中に制約をいったん保存し、後で使用することができます。ただし、複合制約を検索条件のセットとして保存することはできません。詳細については、検索設定の実行と保存(60-1 ページ)を参照してください。

ヒント　侵入イベントがイベント ビューに表示されない場合、選択した時間範囲を調整すると、結果が返される場合があります。古い時間範囲を選択した場合、その時間範囲内のイベントが削除されていることがあります。ルールのしきい値の設定を調整すると、イベントが生成される場合があります。

パケット ビューの使用

ライセンス: Protection

パケット ビューは、侵入イベントを生成したルールをトリガーしたパケットに関する情報を表示します。

ヒント　イベントを検出するデバイスで [パケットの転送(Transfer Packet)] オプションが無効になっている場合、防御センター でのパケット ビューにはパケット情報は含まれません。

パケット ビューは、パケットがトリガーした侵入イベントに関する情報を提供することによって、イベントのタイムスタンプ、メッセージ、分類、優先順位、およびイベントを生成したルール(標準テキスト ルールでイベントが生成された場合)など、特定のパケットがキャプチャされた理由を示します。パケット ビューは、パケットのサイズなど、パケットに関する一般情報も表示します。

さらに、パケット ビューにはパケット内の各層(データ リンク、ネットワーク、およびトランスポート)について説明したセクションと、パケットを構成するバイトについて説明したセクションがあります。システムがパケットを復号化した場合は、復号化されたバイトを表示できます。折りたたまれたセクションを展開すると、詳細情報を参照できます。

(注)　それぞれのポートスキャン イベントは複数のパケットによってトリガーされるため、ポートスキャン イベントは特別なバージョンのパケット ビューを使用します。詳細については、ポートスキャンの検出(34-3 ページ)を参照してください。

次の表に、パケット ビューで実行できる操作を示します。

表 41-5　パケット ビューの操作

目的	操作
パケット ビューで日時範囲を変更する	イベント時間の制約の設定（58-27 ページ）で詳細を参照してください。
パケットのビューに表示される情報について理解する	詳細については、以下を参照してください。 • イベント情報の表示（41-27 ページ） • フレーム情報の表示（41-35 ページ） • データリンク層情報の表示（41-36 ページ） • ネットワーク層情報の表示（41-36 ページ） • トランスポート層情報の表示（41-39 ページ） • パケット バイト情報の表示（41-41 ページ）
後でインシデントに転送できるようにイベントをクリップボードに追加する	次のいずれかを行います。 • [コピー（Copy）] をクリックして、パケットを表示するイベントをコピーします • [すべてをコピー（Copy All）] をクリックして、以前にパケットを選択したすべてのイベントをコピーします クリップボードはユーザごとに最大 25,000 個のイベントを保存します。クリップボードの詳細については、クリップボードの使用（41-54 ページ）を参照してください。
イベント データベースからイベントを削除する	次のいずれかを行います。 • [削除（Delete）] をクリックして、パケットを表示しているイベントを削除します • [すべて削除（Delete All）] をクリックして、以前にパケットを選択したすべてのイベントを削除します
イベントに確認済みのマークを付けて、イベント ビューから削除し、イベント データベースからは削除しない	次のいずれかを行います。 • [確認（Review）] をクリックして、パケットを表示しているイベントを確認します • [すべて確認（Review All）] をクリックして、以前にパケットを選択したすべてのイベントを確認します 詳細については、侵入イベントの確認（41-18 ページ）を参照してください。確認されたイベントは、[侵入イベント統計（Intrusion Event Statistics）] ページのイベント統計情報に引き続き含まれることに注意してください。

表 41-5　パケット ビューの操作（続き）

目的	操作
イベントをトリガーしたパケット（libpcap 形式のパケット キャプチャ ファイル）のローカル コピーをダウンロードする	次のいずれかを行います。 • [パケットのダウンロード（Download Packet）] をクリックして、表示中のイベントのキャプチャされたパケットのコピーを保存します • [すべてのパケットのダウンロード（Download All Packets）] をクリックして、以前にパケットを選択したすべてのイベントのキャプチャされたパケットのコピーを保存します キャプチャされたパケットは libpcap 形式で保存されます。この形式は、複数の一般的なプロトコル アナライザで使用されます。 単一のポートスキャン イベントは複数のパケットに基づいているため、ポートスキャン パケットをダウンロードできないことに注意してください。ただし、ポートスキャン ビューは使用可能なすべてのパケット情報を提供します。詳細については、ポートスキャン イベントについて（34-7 ページ）を参照してください。 ダウンロードするには少なくとも 15 % の利用可能なディスク容量が必要であることに注意してください。
ページ セクションを展開または縮小する	セクションの隣にある矢印をクリックします。

パケット ビューを表示する方法：

アクセス：Admin/Intrusion Admin

手順 1　侵入イベントのテーブル ビューで、表示するパケットを選択します。詳細については、イベントのテーブル ビューのイベントの制約の表を参照してください。

パケット ビューが表示されます。複数のイベントを選択した場合は、ページの下部にあるページ番号を使用してパケットのページ切り替えができます。

イベント情報の表示

ライセンス：Protection

パケット ビューで、[イベント情報（Event Information）] セクションのパケットに関する情報を表示できます。

イベント

イベントのメッセージ。ルールベースのイベントの場合、これはルール メッセージに対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

イベントの ID は、*(GID:SID:Rev)* の形式でメッセージに付加されます。*GID* は、ルール エンジン、デコーダ、またはイベントを生成したプリプロセッサのジェネレータ ID です。*SID* は、ルール、デコーダ メッセージ、またはプリプロセッサ メッセージの識別子です。*Rev* はルールのリビジョン番号です。詳細については、プリプロセッサ ジェネレータ ID の読み取り（41-44 ページ）を参照してください。

Timestamp

パケットがキャプチャされた時間。

分類（Classification）

イベントの分類。ルールベースのイベントの場合、これはルールの分類に対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

[プライオリティ（Priority）]

イベントの優先順位。ルールベースのイベントの場合、これは `priority` キーワードの値または `classtype` キーワードの値に対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

入力セキュリティ ゾーン（Ingress Security Zone）

イベントをトリガーしたパケットの入力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。セキュリティ ゾーンの操作（3-44 ページ）を参照してください。

出力セキュリティ ゾーン（Egress Security Zone）

インライン展開環境の場合、イベントをトリガーしたパケットの出力セキュリティ ゾーン。セキュリティ ゾーンの操作（3-44 ページ）を参照してください。

Device

アクセス コントロール ポリシーが適用された管理対象デバイス。デバイスの管理（4-1 ページ）を参照してください。

セキュリティ コンテキスト（Security Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチ コンテキスト モードの ASA FirePOWER デバイスだけです。

入力インターフェイス（Ingress Interface）

イベントをトリガーしたパケットの入力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列だけに入力されます。センシング インターフェイスの設定（4-66 ページ）を参照してください。

出力インターフェイス（Egress Interface）

インライン セットの場合、イベントをトリガーしたパケットの出力インターフェイス。センシング インターフェイスの設定（4-66 ページ）を参照してください。

送信元/宛先 IP（Source/Destination IP）

イベント（ソース）をトリガーしたパケットの発生元であるホスト IP アドレスまたはドメイン名、またはイベントをトリガーしたトラフィックのターゲット（宛先）ホスト。

ドメイン名を表示するには、IP アドレス解決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、イベント ビュー設定の設定（71-3 ページ）を参照してください。

アドレスまたはドメイン名をクリックしてコンテキスト メニューを表示してから、whois 検索を実行する場合は [Whois（Whois）] を、ホスト情報を表示する場合は [ホスト プロファイルの表示（View Host Profile）] を、アドレスをグローバル ブラックリストまたはホワイトリストに追加する場合は [今すぐブラックリスト（Blacklist Now）] または [今すぐホワイトリスト（Whitelist Now）] を選択します。ホスト プロファイルの使用（49-1 ページ）およびグローバル ホワイトリストおよびブラックリストの操作（3-7 ページ）を参照してください。

送信元ポート/ICMP タイプ（Source Port/ICMP Type）

イベントをトリガーしたパケットの送信元ポート。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP タイプを表示します。

宛先ポート/ICMP コード（Destination Port/ICMP Code）

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP コードを表示します。

電子メールのヘッダー（Email Headers）

電子メール ヘッダーから取得したデータ。電子メール ヘッダーは侵入イベントのテーブル ビューには表示されませんが、電子メール ヘッダー データは検索条件として使用できることに注意してください。

電子メール ヘッダーを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [ヘッダーの記録（Log Headers）] オプションを有効にする必要があります。詳細については、SMTP デコードについて（27-65 ページ）を参照してください。ルールベースのイベントの場合、この行は電子メール データが取得されたときに表示されます。

HTTP ホスト名（HTTP Hostname）

（存在する場合）HTTP 要求のホスト ヘッダーから取得されたホスト名。この行には、最大 256 バイトの完全なホスト名が表示されます。ホスト名が単一行よりも長い場合、展開矢印（  ）をクリックすると完全なホスト名が表示されます。

ホスト名を表示するには、HTTP 検査プリプロセッサの [ホスト名の記録（Log Hostname）] オプションを有効にする必要があります。詳細については、サーバレベル HTTP 正規化オプションの選択（27-36 ページ）を参照してください。

HTTP 要求パケットにホスト名が常に含まれているわけではないことに注意してください。ルールベースのイベントの場合、この行はパケットに HTTP ホスト名または HTTP URI が含まれている場合に表示されます。

HTTP URI

（存在する場合）侵入イベントをトリガーした HTTP 要求パケットに関連付けられた raw URI。この行には、最大 2048 バイトの完全な URI が表示されます。URI が単一行よりも長い場合、展開矢印（  ）をクリックすると完全な URI が表示されます。

URI を表示するには、HTTP 検査プリプロセッサの [URI の記録（Log URI）] オプションを有効にする必要があります。詳細については、サーバレベル HTTP 正規化オプションの選択（27-36 ページ）を参照してください。

HTTP 要求パケットに URI が常に含まれているわけではないことに注意してください。ルールベースのイベントの場合、この行はパケットに HTTP ホスト名または HTTP URI が含まれている場合に表示されます。

HTTP 応答によってトリガーされた侵入イベントの関連 HTTP URI を参照するには、[両ポートでのストリーム リアセンブルの実行（Perform Stream Reassembly on Both Ports）] オプションに HTTP サーバのポートを設定する必要があります。ただし、これにより、トラフィックのリアセンブル用のリソース要求が増加することに注意してください。ストリーム再構成のオプションの選択（29-30 ページ）を参照してください。

侵入ポリシー（Intrusion Policy）

（存在する場合）侵入イベントを生成した侵入、プリプロセッサ、デコーダのルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。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）および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）を参照してください。

アクセス コントロール ポリシー（Access Control Policy）

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効にされた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。アクセス コントロール ポリシーの管理（12-12 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（Access Control Rule）

イベントを生成した侵入ルールと関連付けられたアクセス コントロール ルール。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）を参照してください。[デフォルト アクション（Default Action）] は、ルールが有効にされた侵入ポリシーがアクセス コントロール ルールに関連付けられていないことと、代わりにアクセス コントロール ポリシーのデフォルト アクションとして設定されていることを示します。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）を参照してください。

ルール（Rule）

標準テキスト ルール イベントの場合、イベントを生成したルール。

イベントが、共有オブジェクトのルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

ルール データにはネットワークに関する機密情報が含まれるため、管理者はユーザが View Local Rules 権限を使用してパケット ビューでルール情報を表示できる機能を、ユーザ ロール エディタで切り替えることができます。詳細については、ユーザ特権とオプションの変更（61-59 ページ）を参照してください。

アクション（Actions）

標準テキスト ルール イベントの場合は、[アクション（Actions）] を展開して、イベントをトリガーしたルールに対して次の操作のいずれかを実行します。

- ルールを編集する
- ルールのリビジョンのドキュメンテーションを表示する
- ルールにコメントを追加する
- ルールの状態を変更する
- ルールのしきい値を設定する
- ルールを抑制する

詳細については、パケット ビュー アクションの使用（41-31 ページ）、パケット ビュー内でのしきい値オプションの設定（41-33 ページ）、およびパケット ビュー内での抑制オプションの設定（41-34 ページ）を参照してください。

イベントが、共有オブジェクトのルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

パケット ビュー アクションの使用

ライセンス：Protection

パケット ビューで、イベントをトリガーしたルールの [イベント情報（Event Information）] セクションにあるいくつかのアクションを実行できます。イベントが、共有オブジェクトのルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。ルールのアクションを表示するには、[アクション（Actions）] を展開する必要があります。

編集（Edit）

標準テキスト ルール イベントの場合、[編集（Edit）] をクリックして、イベントを生成したルールを変更します。

イベントが、共有オブジェクトのルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

（注） シスコによって提供された（カスタム標準テキスト ルールではない）ルールを編集する場合、実際には新規のローカル ルールを作成していることになります。ローカル ルールを設定して、イベントを生成し、現在の侵入ポリシーで元のルールを無効にしていることを確認してください。ただし、デフォルトのポリシーのローカル ルールは有効に**できない**ことに注意してください。詳細については、既存のルールの変更（36-114 ページ）を参照してください。

ドキュメントの表示（View Documentation）

標準テキスト ルール イベントの場合、[ドキュメントの表示（View Documentation）] をクリックして、イベントを生成したルール リビジョンの説明を確認します。

ルールのコメント（Rule Comment）

標準テキスト ルール イベントの場合、[ルールのコメント（Rule Comment）] をクリックして、イベントを生成したルールにテキスト コメントを追加します。

これにより、ルールや、特定されたエクスプロイトまたはポリシー違反に関するコンテキストおよび情報を提供できます。さらに、ルール エディタでルールのコメントの追加および表示を行うこともできます。詳細については、ルールへのコメントの追加（36-115 ページ）を参照してください。

このルールを無効にする（Disable this rule）

このイベントが標準テキスト ルールによって生成された場合は、必要に応じてルールを無効にできます。ローカルで編集できるすべてのポリシーにルールを設定できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

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。

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、シスコが提供するデフォルト ポリシーは編集できません。

（注） パケット ビューから共有オブジェクトのルールを無効にしたり、デフォルトのポリシーでルールを無効にしたりすることは**できません**。

イベントを生成するようにこのルールを設定する（Set this rule to generate events）

このイベントが標準テキスト ルールによって生成された場合は、ルールを設定して、ローカルで編集できるすべてのポリシーでイベントを生成できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

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。

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、シスコが提供するデフォルト ポリシーは編集できません。

（注）　パケット ビューからイベントを生成するように共有オブジェクトのルールを設定したり、デフォルト ポリシーのルールを無効にしたりすることは**できません**。

ドロップするようにこのルールを設定する（Set this rule to drop）

管理対象デバイスがネットワーク上でインライン展開されている場合、イベントをトリガーしたルールを設定して、ローカルで編集できるすべてのポリシーでルールをトリガーするパケットをドロップできます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、シスコが提供するデフォルト ポリシーは編集できません。このオプションは [インライン時にドロップ（Drop when Inline）] が現在のポリシーで有効になっている場合のみ表示されることに注意してください。詳細については、インライン展開でのドロップ動作の設定（31-6 ページ）を参照してください。

しきい値オプションを設定する（Set Thresholding Options）

このオプションを使用して、ローカルで編集できるすべてのポリシーで、これをトリガーしたルールのしきい値を作成できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）でのみしきい値を作成することもできます。

しきい値オプションについては、パケット ビュー内でのしきい値オプションの設定（41-33 ページ）で説明します。

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーは編集できますが、シスコが提供するデフォルトの侵入ポリシーは編集できません。

抑制オプションを設定する（Set Suppression Options）

このオブジェクトを使用して、ローカルで編集できるすべてのポリシーで、このイベントをトリガーしたルールを抑制できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみでルールを制約することもできます。

抑制オプションについては、パケット ビュー内での抑制オプションの設定（41-34 ページ）で説明します。

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、シスコが提供するデフォルト ポリシーは編集できません。

パケット ビュー内でのしきい値オプションの設定

ライセンス：Protection

侵入イベントのパケット ビューでしきい値オプションを設定することによって、ルールごとに、時間の経過とともに生成されるイベントの数を制御できます。ローカルで編集できるすべてのポリシーに、またはローカルで編集できる場合は現在のポリシー（つまり、イベントを生成したポリシー）のみに、しきい値オプションを設定できます。

パケット ビュー内でしきい値オプションを設定する方法：

アクセス：Admin/Intrusion Admin

手順 1　侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報（Event Information）] セクションの [アクション（Actions）] を展開し、[しきい値オプションを設定する（Set Thresholding Options）] を展開し、次の 2 つのオプションのいずれかを選択します。

- **現在のポリシーにおいて（in the current policy）**
- **ローカルで作成されたすべてのポリシーにおいて（in all locally created policies）**

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、シスコが提供するデフォルト ポリシーは編集できません。

しきい値オプションが表示されます。

手順 2　設定するしきい値の種類を選択します。

- 指定された期間あたりのイベント インスタンス数に通知を制限する場合は、[制限（Limit）] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[しきい値（Threshold）] を選択します。
- 指定されたイベント インスタンス数後に期間あたり 1 回ずつ通知を提供する場合は、[両方（Both）] を選択します。

手順 3　イベント インスタンスを [送信元（Source）] または [宛先（Destination）] IP アドレスでトラックするかどうかを示すために、該当するラジオ ボタンを選択します。

手順 4　[カウント（Count）] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

手順 5　[秒（Seconds）] フィールドで、イベント インスタンスをトラックする期間を指定する 1 から 86400 までの数を入力します。

手順 6　既存の侵入ポリシーでこのルールの現在のしきい値をオーバーライドする場合、[このルールの既存の設定をオーバーライドする（Override any existing settings for this rule）] を選択します。

手順 7　[しきい値の保存（Save Thresholding）] をクリックします。

システムはしきい値を追加し、成功を示すメッセージを表示します。既存の設定をオーバーライドしない選択をした場合に競合が発生すると、競合を通知するメッセージが表示されます。

パケット ビュー内での抑制オプションの設定

ライセンス：Protection

抑制オプションを使用して、侵入イベントをまとめて、または発信元 IP アドレスまたは宛先 IP アドレスに基づいて抑制できます。ローカルで編集できるすべてのポリシーで抑制オプションを設定できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみに抑制オプションを設定することもできます。

パケット ビュー内で侵入イベントを抑制する方法：

アクセス：Admin/Intrusion Admin

手順 1　侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報（Event Information）] セクションの [アクション（Actions）] を展開し、[抑制オプションを設定する（Set Suppression Options）] を展開し、次の 2 つのオプションのいずれかをクリックします。

- **現在のポリシーにおいて（in the current policy）**
- **ローカルで作成されたすべてのポリシーにおいて（in all locally created policies）**

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、シスコが提供するデフォルト ポリシーは編集できません。

抑制オプションが表示されます。

手順 2　次のいずれかの [追跡対象（Track By）] オプションを選択します。

- このイベントをトリガーしたルールのイベントを完全に抑制するには、[ルール（Rule）] を選択します。
- 指定した送信元 IP アドレスから発信されたパケットによって生成されるイベントを抑制するには、[送信元（Source）] を選択します。
- 指定した宛先 IP アドレスに入るパケットによって生成されるイベントを抑制するには、[宛先（Destination）] を選択します。

手順 3　[IP アドレス（IP address）] または [CIDR ブロック（CIDR block）] フィールドで、発信元または宛先 IP アドレスとして指定する IP アドレスまたは CIDR ブロック/プレフィックス長を入力します。

FireSIGHT システムで CIDR 表記およびプレフィッ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 4　[抑制の保存（Save Suppression）] をクリックします。

侵入ポリシー内の抑制オプションは、ユーザの仕様に従って変更されます。既存の設定をオーバーライドしない選択をした場合に競合が発生すると、競合を通知するメッセージが表示されます。

フレーム情報の表示

ライセンス：Protection

パケット ビューで、[フレーム（Frame）] の横にある矢印をクリックして、キャプチャされたフレームに関する情報を表示します。パケット ビューには単一フレームまたは複数フレームを表示できます。各フレームには、個々のネットワーク パケットに関する情報が表示されます。たとえば、タグ付きパケットまたはリアセンブルされた TCP ストリーム内のパケットの場合、複数のフレームが表示されます。タグ付きパケットの詳細については、攻撃後トラフィックの評価（36-98 ページ）を参照してください。リアセンブルされた TCP ストリームの詳細については、TCP ストリームの再構成（29-30 ページ）を参照してください。

フレーム n（Frame n）
キャプチャされたフレーム。*n* は単一フレーム パケットの場合は 1、複数フレーム パケットの場合は増分フレーム番号です。フレーム内のキャプチャされたバイト数はフレーム番号に追加されます。

到着時間（Arrival Time）
フレームがキャプチャされた日時。

前のフレームがキャプチャされてからの時間（Time delta from previous captured frame）
複数フレーム パケットの場合、前のフレームがキャプチャされてからの経過時間。

前のフレームが表示されてからの時間（Time delta from previous displayed frame）
複数フレーム パケットの場合、前のフレームが表示されてからの経過時間。

参照または最初のフレームからの時間（Time since reference or first frame）
複数フレーム パケットの場合、最初のフレームがキャプチャされてからの経過時間。

フレーム番号（Frame Number）
増分フレーム番号。

フレーム長（Frame Length）
フレームの長さ（バイト単位）。

キャプチャ長（Capture Length）
キャプチャされたフレームの長さ（バイト単位）。

フレームのマーク付け（Frame is marked）
フレームがマークされているかどうか（true または false）。

フレームのプロトコル（Protocols in frame）
フレームに含まれるプロトコル。

データリンク層情報の表示

ライセンス：Protection

パケット ビューで、データリンク層プロトコル（**イーサネット II** など）の横にある矢印をクリックして、パケットに関するデータリンク層情報を表示します。この情報には、送信元ホストと宛先ホストの 48 ビットの Media Access Control（MAC）アドレスが含まれています。ハードウェア プロトコルに応じて、パケットに関する他の情報も表示されることがあります。

（注） この例では、イーサネット リンク層情報について説明していることに注意してください。他のプロトコルも表示されることがあります。

パケット ビューはデータリンク層で使用されるプロトコルを反映します。次のリストでは、パケット ビューでイーサネット II または IEEE 802.3 イーサネット パケットについて参照できる情報について説明します。

[接続先（Destination）]

宛先ホストの MAC アドレス。

（注） イーサネットは、宛先アドレスとしてマルチキャストおよびブロードキャスト アドレスを使用することもできます。

ソース（Source）

送信元ホストの MAC アドレス。

タイプ（Type）

イーサネット II パケットの場合、イーサネット フレームでカプセル化されるパケットの種類。たとえば、IPv6 または ARP データグラム。この項目はイーサネット II パケットの場合にのみ表示されることに注意してください。

長さ（Length）

IEEE 802.3 イーサネット パケットの場合、チェックサムを含まないパケットのトータル長（バイト単位）。この項目は IEEE 802.3 イーサネット パケットの場合にのみ表示されることに注意してください。

ネットワーク層情報の表示

ライセンス：Protection

パケット ビューで、ネットワーク層プロトコル（たとえば、[インターネット プロトコル（Internet Protocol）]）の横にある矢印をクリックして、パケットに関連したネットワーク層の情報の詳細を表示します。

（注） この例では、IP パケットについて説明していることに注意してください。他のプロトコルも表示されることがあります。

詳細については、次の各項を参照してください。

- IPv4 ネットワーク層情報の表示（41-37 ページ）
- IPv6 ネットワーク層情報の表示（41-38 ページ）

IPv4 ネットワーク層情報の表示

ライセンス：Protection

以下のリストは、IPv4 パケットで表示される可能性があるプロトコル固有の情報の説明です。

バージョン（Version）
インターネット プロトコルのバージョン番号。

ヘッダー長（Header Length）
すべての IP オプションを含む、ヘッダーのバイト数。オプションのない IP ヘッダーの長さは 20 バイトです。

差別化サービス（Differentiated Services）フィールド
送信元ホストが明示的輻輳通知（ECN）をサポートする方法を示す、差別化サービスの値。

- `0x0`：ECN-Capable Transport（ECT）をサポートしません。
- `0x1` および `0x2`：ECT をサポートします
- `0x3`：Congestion Experienced（CE）

トータル長（Total Length）
IP ヘッダーを差し引いた IP パケットの長さ（バイト単位）。

ID
送信元ホストから送信される IP データグラムを一意に識別する値。この値は同じデータグラム フラグメントをトレースするために使用されます。

フラグ（Flags）
IP フラグメンテーションを制御する値。

[最終フラグメント（Last Fragment）] フラグの値は、データグラムに関連付けられた追加のフラグメントが存在するかどうかを次のように示します。

- `0`：データグラムに関連付けられた追加のフラグメントは存在しない
- `1`：データグラムに関連付けられた追加のフラグメントが存在する

[フラグメント化しない（Don’t Fragment）] フラグの値は、データグラムをフラグメント化できるかどうかを次のように制御します。

- `0`：データグラムをフラグメント化できる
- `1`：データグラムをフラグメント化**してはならない**

フラグメント オフセット（Fragment Offset）
データグラムの先頭からのフラグメント オフセットの値。

存続時間（ttl）（Time to Live (ttl)）
データグラムが期限切れになる前にデータグラムがルータ間で作成できるホップの残数。

プロトコル

IP データグラムにカプセル化されるトランスポート プロトコル。たとえば、ICMP、IGMP、TCP、または UDP。

ヘッダー チェックサム（Header Checksum）

IP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損したか、侵入回避の試行において使用中である可能性があります。

送信元/宛先（Source/Destination）

送信元（または宛先）ホストの IP アドレスまたはドメイン名。

ドメイン名を表示するには、IP アドレス解決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、イベント ビュー設定の設定（71-3 ページ）を参照してください。

アドレスまたはドメイン名をクリックしてコンテキスト メニューを表示してから、whois 検索を実行する場合は [Whois（Whois）] を、ホスト情報を表示する場合は [ホスト プロファイルの表示（View Host Profile）] を、アドレスをグローバル ブラックリストまたはホワイトリストに追加する場合は [今すぐブラックリスト（Blacklist Now）] または [今すぐホワイトリスト（Whitelist Now）] を選択します。ホスト プロファイルの使用（49-1 ページ） およびグローバル ホワイトリストおよびブラックリストの操作（3-7 ページ）を参照してください。

IPv6 ネットワーク層情報の表示

ライセンス：Protection

以下のリストは、IPv6 パケットで表示される可能性があるプロトコル固有の情報の説明です。

トラフィック クラス（Traffic Class）

IPv6 パケットのクラスまたは優先順位を識別するための IPv6 ヘッダーの試験的な 8 ビット フィールド。IPv4 で提供される差別化サービス機能に類似しています。未使用の場合、このフィールドはゼロに設定されます。

フロー ラベル（Flow Label）

非デフォルトの QoS やリアルタイム サービスなど、特別なフローを識別するオプションの 20 ビット IPv6 16 進数値（1 ～ FFFF）。未使用の場合、このフィールドはゼロに設定されます。

ペイロード長（Payload Length）

IPv6 ペイロードのオクテットの数を特定する 16 ビット フィールド。このフィールドは、拡張ヘッダーなど、IPv6 ヘッダーに続くすべてのパケットから構成されます。

次ヘッダー（Next Header）

IPv6 ヘッダーのすぐ後に続く、ヘッダーの種類を特定する 8 ビットのフィールド。IPv4 プロトコル フィールドと同じ値が使用されます。

ホップ リミット（Hop Limit）

パケットを転送するノードごとに 1 つずつデクリメントする 8 ビットの 10 進整数。デクリメントした値がゼロになると、パケットは破棄されます。

ソース（Source）

送信元ホストの 128 ビットの IPv6 アドレス。

[接続先（Destination）]
宛先ホストの 128 ビットの IPv6 アドレス。

トランスポート層情報の表示

ライセンス：Protection

パケット ビューで、トランスポート層プロトコル（たとえば [TCP]、[UDP]、または [ICMP]）の横にある矢印をクリックして、パケットに関する詳細情報を表示します。

ヒント　（存在する場合）[データ（Data）] をクリックして、パケット ビューの [パケット情報（Packet Information）] セクションで、プロトコルのすぐ上にあるペイロードの最初の 24 バイトを表示します。

次の各プロトコルのトランスポート層の内容は、以下で説明されています。

- TCP パケット ビュー（41-39 ページ）
- UDP パケット ビュー（41-40 ページ）
- ICMP パケット ビュー（41-40 ページ）

（注）　これらの例では、TCP、UDP、および ICMP パケットについて説明していることに注意してください。他のプロトコルも表示されることがあります。

TCP パケット ビュー

ライセンス：Protection

この項では、TCP パケットのプロトコル固有の情報について説明します。

ソース ポート
発信元のアプリケーション プロトコルを識別する番号。

接続先ポート（Destination port）
受信側のアプリケーション プロトコルを識別する番号。

シーケンス番号（Sequence number）
TCP ストリームの初期シーケンス番号と連動する、現在の TCP セグメントの最初のバイトの値。

次のシーケンス番号（Next sequence number）
応答パケットにおける、送信する次のパケットのシーケンス番号。

確認応答番号（Acknowledgement number）
以前に受信されたデータのシーケンス番号に連動した TCP 確認応答。

ヘッダー長（Header Length）
ヘッダーのバイト数。

フラグ(Flags)

TCP セグメントの伝送状態を示す 6 ビット。

- U:緊急ポインタが有効
- A:確認応答番号が有効
- P:受信者はデータをプッシュする必要がある
- R:接続をリセットする
- S:シーケンス番号を同期して新しい接続を開始する
- F:送信者はデータ送信を終了した

ウィンドウ サイズ(Window size)

受信ホストが受け入れる、確認応答されていないデータの量(バイト単位)。

チェックサム(Checksum)

TCP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損したか、回避の試行において使用中である可能性があります。

緊急ポインタ(Urgent Pointer)

緊急データが終了する TCP セグメントの位置(存在する場合)。U フラグとともに使用します。

オプション(Options)

TCP オプションの値(存在する場合)。

UDP パケット ビュー

ライセンス: Protection

この項では、UDP パケットのプロトコル固有の情報について説明します。

ソース ポート

発信元のアプリケーション プロトコルを識別する番号。

接続先ポート(Destination port)

受信側のアプリケーション プロトコルを識別する番号。

長さ(Length)

UDP ヘッダーとデータを組み合わせた長さ。

チェックサム(Checksum)

UDP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損した可能性があります。

ICMP パケット ビュー

ライセンス: Protection

この項では、ICMP パケットのプロトコル固有の情報について説明します。

タイプ(Type)

ICMP メッセージのタイプ。

- 0:エコー応答
- 3:宛先到達不能
- 4:ソース クエンチ(始点抑制要求)
- 5:リダイレクト
- 8:エコー要求
- 9:ルータ アドバタイズメント
- 10:ルータ送信要求
- 11:時間超過
- 12:パラメータの問題
- 13:タイムスタンプ要求
- 14:タイムスタンプ応答
- 15:情報要求(廃止)
- 16:情報応答(廃止)
- 17:アドレス マスク要求
- 18:アドレス マスク応答

コード(Code)

ICMP メッセージ タイプに付随するコード。ICMP メッセージ タイプ 3、5、11、および 12 には、RFC 792 で説明されている対応コードがあります。

チェックサム(Checksum)

ICMP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損した可能性があります。

パケット バイト情報の表示

ライセンス: Protection

パケット ビューで、[パケット バイト(Packet Bytes)] の横にある矢印をクリックして、パケットを構成するバイトの 16 進数および ASCII バージョンを表示します。システムがトラフィックを復号した場合は、復号されたパケット バイトを表示できます。

影響レベルを使用してイベントを評価する

ライセンス: Protection

イベントがネットワークに与える影響を評価するために、防御センター は侵入イベントのテーブル ビューに影響レベルを表示します。イベントごとに、防御センター は影響レベル アイコンを追加し、侵入データ、ネットワーク検出データ、脆弱性情報との相関を色で示します。

(注) NetFlow データに基づいてネットワーク マップに追加されたホストで使用可能なオペレーティング システム情報が存在しない場合、ホスト入力機能を使用してホストのオペレーティング システムのアイデンティティを手動で設定しない限り、防御センター はこれらのホストに関係した侵入イベントに対して影響レベル [脆弱(Vulnerable)](影響レベル 1:赤)を割り当てることはできません。

次の表に、影響レベルで使用可能な値を示します。

表 41-6　影響レベル

影響レベル	脆弱性	カラー	説明
0	不明	グレー	送信元ホストと宛先ホストは両方ともネットワーク検出によってモニタされているネットワーク上に存在しません。
1	脆弱	赤色	次のいずれかを行います。 • 送信元ホストまたは宛先ホストはネットワーク マップ内にあり、脆弱性はホストにマッピングされます • 送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵害される可能性があります。詳細については、影響レベル 1 の設定(36-50 ページ)を参照してください。
2	潜在的に脆弱	オレンジ	送信元ホストまたは宛先ホストはネットワーク マップ内にあり、次のいずれかに当てはまります。 • ポート指向のトラフィックの場合、ポートはサーバ アプリケーション プロトコルを実行しています • ポート指向ではないトラフィックの場合、ホストはプロトコルを使用します
3	現在は脆弱ではない	黄色	送信元ホストまたは宛先ホストはネットワーク マップ内にあり、次のいずれかに当てはまります。 • ポート指向のトラフィック(TCP や UDP など)の場合、ポートは開いていません • ポート指向ではないトラフィック(ICMP など)の場合、ホストはプロトコルを使用しません
4	不明なターゲット	青	送信元ホストまたは宛先ホストがモニタ対象のネットワークにありますが、ネットワーク マップ内にそのホストのエントリがありません。

テーブル ビューの影響レベルを使用してイベントを評価する方法:

アクセス: Admin/Intrusion Admin

手順 1　[分析(Analysis)] > [侵入(Intrusions)] > [イベント(Events)] を選択します。

デフォルトの侵入イベントのワークフローの最初のページが表示されます。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定(71-3 ページ)を参照してください。イベントが表示されない場合は、時間範囲の調整が必要な可能性があります。イベント時間の制約の設定(58-27 ページ)を参照してください。

手順 2　評価するイベントのみを表示するには、イベント ビューを制約します。

詳細については、ドリルダウン ページとテーブル ビュー ページの使用(41-21 ページ)を参照してください。

手順 3　ページの上部にある [イベントのテーブル ビュー(Table View of Events)] をクリックします。

イベントのテーブル ビューが表示されます。[影響(Impact)] には、影響レベルの表に記載されているいずれかの値が入ります。

手順 4　影響レベルでテーブルをソートするには、[影響(Impact)] をクリックします。

イベントは影響レベルでソートされます。

ヒント　ソート順序を反転させるには、もう一度 [影響(Impact)] をクリックします。

プリプロセッサ イベントの読み取り

ライセンス: Protection

プリプロセッサは 2 つの機能を備えています。指定されたアクション(HTTP トラフィックのデコードや正規化など)をパケットに対して実行する機能と、指定されたプリプロセッサ オプションの実行をレポートする機能です。これは、関連するプリプロセッサ ルールが有効になっている場合、パケットによって指定のプリプロセッサ オプションがトリガーされたときに、常にイベントを生成することによって実現されます(たとえば、HTTP Inspect ジェネレータ(GID)119 と Snort ID(SID)2 に関連するプリプロセッサ ルールと、[二重エンコード(Double Encoding)] HTTP Inspect オプションを有効にすると、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、攻撃者は重複している IP フラグメントを作成して、ホスト上で DoS 攻撃を引き起こす可能性があります。IP 最適化のプリプロセッサはこのタイプの攻撃を検出し、それに関する侵入イベントを生成できます。

詳細については、次の各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(41-44 ページ)では、プリプロセッサで生成されたイベントに含まれる情報について説明しています。
- プリプロセッサ ジェネレータ ID の読み取り(41-44 ページ)では、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述します。

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、パケット ディスプレイにイベントの詳細なルールの説明が含まれていないという点で、ルール イベントとは異なります。代わりに、パケット ディスプレイには、イベント メッセージ、ジェネレータ ID、Snort ID、パケット ヘッダー データおよびパケット ペイロードが表示されます。これにより、パケットのヘッダー情報を分析し、そのヘッダー オプションが使用中かどうか判断し、それがシステムをエクスプロイトする可能性がある場合は、パケット ペイロードを検査できます。プリプロセッサによる各パケットの分析が完了すると、ルール エンジンは、パケットに対して適切なルールを実行し（プリプロセッサが各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 レベルの脅威についてさらに分析を行い、それらのパケットについてレポートします。

プリプロセッサ 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、パケットによってトリガーされたプリプロセッサを示す独自のジェネレータ ID 番号、つまり GID があります。一部のプリプロセッサには関連した SID もあります。これは、潜在的な攻撃を分類する ID 番号です。これにより、ルールの Snort ID（SID）がルールをトリガーするパケットのコンテキストを提供するのとほぼ同じ方法で、イベントのタイプを分類することによって、より効率的にイベントを解析できます。侵入ポリシーの [ルール（Rules）] ページでは、[プリプロセッサ（Preprocessors）] フィルタ グループでプリプロセッサ別にプリプロセッサ ルールを一覧表示できます。また、プリプロセッサのプリプロセッサ ルールや [大項目（Category）] フィルタ グループのパケット デコーダ サブグループを一覧表示することもできます。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）と表 32-1（32-2 ページ）を参照してください。

（注）　標準テキスト ルールによって生成されたイベントのジェネレータ ID は 1 です。イベントの SID は、トリガーされた特定のルールを示します。共有オブジェクトのルールの場合、イベントにはジェネレータ ID 3 と、トリガーされた特定のルールを示す SID が含まれます。

次の表に、各 GID を生成するイベントの種類を示します。

表 41-7　ジェネレータ ID

ID	コンポーネント	説明	詳細
1	標準テキスト ルール	イベントは、パケットが標準テキスト ルールをトリガーしたときに生成されました。	表 32-1（32-2 ページ）
2	タグ付きパケット	イベントは、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生成されました。これは、[タグ（tag）] ルール オプションが使用された場合に発生します。	攻撃後トラフィックの評価（36-98 ページ）
3	共有オブジェクト ルール	イベントは、パケットが共有オブジェクトのルールをトリガーしたときに生成されました。	表 32-1（32-2 ページ）
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。	HTTP トラフィックのデコード（27-34 ページ）

表 41-7　ジェネレータ ID (続き)

ID	コンポーネント	説明	詳細
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。	Back Orifice の検出 (34-2 ページ)
106	RPC デコーダ	RPC デコーダがパケットを復号化しました。	Sun RPC プリプロセッサの使用 (27-50 ページ)
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。	パケットのデコードについて (29-18 ページ)
119、120	HTTP 検査プリプロセッサ	イベントは HTTP 検査プリプロセッサによって生成されました。GID 120 ルールは、サーバ固有の HTTP トラフィックに関するルールです。	HTTP トラフィックのデコード (27-34 ページ)
122	ポートスキャン ディテクタ	イベントはポートスキャン フロー ディテクタによって生成されました。詳細を参照してください。	ポートスキャンの検出 (34-3 ページ)
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。	IP パケットの最適化 (29-13 ページ)
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。	SMTP デコードについて (27-65 ページ)
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。	サーバレベルの FTP オプションについて (27-24 ページ) クライアントレベルの FTP オプションについて (27-30 ページ)
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。	FTP および Telnet トラフィックのデコード (27-20 ページ)
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。	SSH プロプロセッサによるエクスプロイトの検出 (27-73 ページ)
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。	TCP ストリームの前処理の使用 (29-22 ページ)
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。	DNS ネーム サーバ応答におけるエクスプロイトの検出 (27-16 ページ)
133	DCE/RPC プリプロセッサ	このイベントは、DCE/RPC プリプロセッサにより生成されました。	DCE/RPC トラフィックのデコード (27-2 ページ)
134	ルール遅延 パケット遅延	ルールの遅延によって侵入ルールのグループが中断 (134:1) または再有効化 (134:2) されたとき、またはパケットの遅延しきい値に達したためにシステムがパケットの検査を停止 (134:3) したときに、イベントが生成されました。	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)
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のホストに対する過度の識別したときに、イベントが生成されました。	レート ベース攻撃の防止 (34-10 ページ)

表 41-7　ジェネレータ ID (続き)

ID	コンポーネント	説明	詳細
138、139	センシティブ 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。	センシティブ データの検出 (34-20 ページ)
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。	Session Initiation Protocol のデコード (27-52 ページ)
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。	IMAP トラフィックのデコード (27-58 ページ)
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。	POP トラフィックのデコード (27-62 ページ)
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。	GTP コマンド チャネルの設定 (27-57 ページ)
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。	Modbus プリプロセッサの設定 (28-1 ページ)
145	DNP3 プリプロセッサ	イベントは DNP3 SCADA プリプロセッサによって生成されました。	DNP3 プリプロセッサの設定 (28-3 ページ)

侵入イベントの検索

ライセンス: Protection

FireSIGHT システムで配信された定義済み検索を使用するか、または独自の検索基準を作成することによって特定の侵入イベントを検索できます。

定義済み検索は例として使用でき、これによりネットワークに関する重要な情報に素早くアクセスできます。デフォルトの検索内の特定のフィールドを変更して、使用するネットワーク環境に合わせてカスタマイズし、後で再利用できるようにそれらを保存することもできます。覚えておくべき点として、検索結果は、検索するイベントの使用可能なデータに依存します。つまり、使用可能なデータによっては、検索の制約が適用されないことがあります。たとえば、復号されたトラフィックでトリガーされた侵入イベントだけが SSL 情報を含んでいます。

ヒント　侵入イベント検索で IP アドレスとポートを指定するための構文の詳細については、検索での IP アドレスの指定 (60-6 ページ) および検索でのポートの指定 (60-8 ページ) を参照してください。

保存されている検索をロードおよび削除する方法など、検索の詳細については、イベントの検索 (60-1 ページ) を参照してください。

使用できる検索条件を以下に示します。

[プライオリティ (Priority)]

表示するイベントのプライオリティを指定します。プライオリティは、`priority` キーワードの値または `classtype` キーワードの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。有効な値は、[高 (high)]、[中 (medium)]、および [低 (low)] です。

影響（Impact）

侵入データとネットワーク検出データの相互関係に基づいて、侵入イベントに割り当てる影響レベルを指定します。大文字と小文字を区別しない有効な値は、`Impact 0`、`Impact Level 0`、`Impact 1`、`Impact Level 1`、`Impact 2`、`Impact Level 2`、`Impact 3`、`Impact Level 3`、`Impact 4`、および `Impact Level 4` です。

影響アイコンの色または部分文字列は使用しないでください（たとえば、`blue`、`level 1`、または `0` を使用しないでください）。

詳細については、影響レベルを使用してイベントを評価する（41-41 ページ）を参照してください。

インライン結果（Inline Result）

次のいずれかを入力してください。

- `dropped`。パケットがインライン展開環境でパケットをドロップするかどうかを指定します
- `would have dropped`。インライン展開環境でパケットをドロップするように侵入ポリシーが設定されている場合に、パケットをドロップするかどうかを指定します

侵入ポリシーのルールの状態またはインライン ドロップ動作にかかわらず、インライン インターフェイスがタップ モードになっている場合を含め、パッシブ展開環境ではシステムはパケットをドロップしないことに注意してください。

ソース IP

侵入イベントに関連する送信元ホストが使用する IP アドレスを指定します。

宛先 IP（Destination IP）

侵入イベントに関連する宛先ホストが使用する IP アドレスを指定します。

送信元/宛先 IP（Source/Destination IP）

侵入イベントを表示するホストによって使用される送信元または宛先 IP アドレスを指定します。

送信元の国（Source Country）

侵入イベントに関連する送信元ホストの国を指定します。

宛先の国（Destination Country）

侵入イベントに関連する宛先ホストの国を指定します。

送信元/宛先の国（Source/Destination Country）

表示する侵入イベントに関連する送信元または宛先ホストの国を指定します。

送信元の大陸（Source Continent）

侵入イベントに関連する送信元ホストの大陸を指定します。

宛先の大陸（Destination Continent）

侵入イベントに関連する宛先ホストの大陸を指定します。

送信元/宛先の大陸（Source/Destination Continent）

表示する侵入イベントに関連する送信元または宛先ホストの大陸を指定します。

元のクライアント IP（Original Client IP）

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーから取得された、元のクライアント IP アドレスを指定します。侵入イベントのこのフィールドの値を取得するには、HTTP プリプロセッサの [クライアントのオリジナル IP アドレスの抽出（Extract Original Client IP Address）] オプションを有効にする必要があります。オプションで、ネットワーク分析ポリシーの同じエリアで、最大 6 つのカスタム クライアント IP ヘッダーを指定し、システムによって [元のクライアント IP（Original Client IP）] イベント フィールドの値が選択される優先順位を設定します。詳細については、サーバレベル HTTP 正規化オプションの選択（27-36 ページ）を参照してください。

プロトコル

http://www.iana.org/assignments/protocol-numbers に一覧表示されている、接続で使用するトランスポート プロトコルの名前または番号を入力します。

侵入イベントのテーブル ビューには [プロトコル（Protocol）] 列がないことに注意してください。これは、送信元および宛先ポート/ICMP の列と関連付けられたプロトコルです。

送信元ポート/ICMP タイプ（Source Port / ICMP Type）

侵入イベントに関連する送信元ポートを指定します。

ヒント　ICMP トラフィックの場合、ポートをターゲットとしないため、このフィールドを使用して特定の ICMP タイプのイベントを検索することができます。

宛先ポート/ICMP コード（Destination Port / ICMP Code）

侵入イベントに関連する宛先ポートを指定します。

ヒント　ICMP トラフィックの場合、ポートをターゲットとしないため、このフィールドを使用して特定の ICMP コードのイベントを検索することができます。

VLAN ID（Admin. VLAN ID）

侵入イベントをトリガーしたパケットに関連付けられている最内部 VLAN ID を指定します。

MPLS ラベル（MPLS Label）

侵入イベントをトリガーしたパケットに関連付けられているマルチプロトコル ラベル スイッチング ラベルを指定します。

メッセージ（Message）

表示するイベントのイベント メッセージのすべてまたは一部を指定します。

分類（Classification）

表示するイベントを生成したルールの分類番号を入力するか、分類名または説明のすべてまたは一部を入力します。番号、名前、または説明をカンマで区切ったリストを入力することもできます。さらに、カスタム分類を追加した場合、その名前または説明のすべてまたは一部を使用して検索することもできます。分類の番号、名前、および説明のリストについては、ルールの分類の表を参照してください。

ジェネレータ（Generator）

表 41-7（41-44 ページ）に示されている、表示するイベントを生成したコンポーネントを指定します。

Snort ID

イベントを生成したルールの Snort ID（SID）を指定するか、オプションで、ルールの複合ジェネレータ ID（GID）および SID を指定します。ここで、GID および SID は、コロン（:）で区切られ、GID:SID の形式になります。次の表の任意の値を指定できます。

表 41-8　Snort ID の検索値

値	例
単一の SID	10000
SID の範囲	10000 ～ 11000
SID より大きい	>10000
SID 以上	>=10000
SID 未満	<10000
SID 以下	<=10000
SID のカンマ区切りリスト	10000,11000,12000
単一の GID:SID の組み合わせ	1:10000
GID:SID の組み合わせのカンマ区切りリスト	1:10000,1:11000,1:12000
SID および GID:SID の組み合わせのカンマ区切りリスト	10000,1:11000,12000

詳細については、プリプロセッサ ジェネレータ ID の読み取り（41-44 ページ）を参照してください。

Snort ID 列は検索結果に表示されないことに注意してください。ユーザが表示するイベントの SID は [メッセージ（Message）] 列にリストされます。

送信元ユーザ（Source User）

送信元ホストにログインしているユーザのユーザ ID を指定します。

宛先ユーザ（Destination User）

宛先ホストにログインしているユーザのユーザ ID を指定します。

送信元/宛先ユーザ（Source/Destination User）

送信元または宛先ホストにログインしているユーザのユーザ ID を指定します。

アプリケーション プロトコル（Application Protocol）

侵入イベントをトリガーしたトラフィックで検出された、ホスト間の通信を表すアプリケーション プロトコルの名前を入力します。

クライアント（Client）

侵入イベントをトリガーしたトラフィックで検出されたモニタ対象のホストで実行されているソフトウェアを表す、クライアント アプリケーションの名前を入力します。

Web アプリケーション（Web Application）

侵入イベントをトリガーしたトラフィックで検出された HTTP トラフィックの内容または要求された URL を表す、Web アプリケーションの名前を入力します。

大項目、タグ（アプリケーション プロトコル、クライアント、Web アプリケーション）（Category, Tag (Application Protocol, Client, Web Application)）

セッションで検出されたアプリケーションに関連するカテゴリまたはタグを入力します。複数のカテゴリまたはタグを指定する場合はカンマで区切ります。これらのフィールドでは、大文字と小文字は区別されません。

アプリケーションのリスク（Application Risk）

セッションで検出されたアプリケーションに関連する最も高いリスクを入力します。有効な条件は次のとおりです。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、および [非常に低い（Very Low）]。これらのフィールドでは、大文字と小文字は区別されません。

ビジネスとの関連性（Business Relevance）

セッションで検出されたアプリケーションに関連する最も低いビジネスとの関連性を入力します。有効な条件は次のとおりです。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、および [非常に低い（Very Low）]。これらのフィールドでは、大文字と小文字は区別されません。

セキュリティ ゾーン（入力、出力、入力/出力）（Security Zone (Ingress、Egress、Ingress/Egress)）

イベントをトリガーしたパケットと関連付けられたセキュリティ ゾーンの名前を指定します。これらのフィールドでは、大文字と小文字は区別されません。セキュリティ ゾーンの操作（3-44 ページ）を参照してください。

Device

アクセス コントロール ポリシーが適用された特定のデバイスに限定して検索するには、デバイス名または IP アドレス、デバイス グループ、スタック、またはクラスタ名を入力します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、検索でのデバイスの指定（60-7 ページ）を参照してください。

スタック構成設定では、プライマリ デバイスとセカンダリ デバイスは、侵入イベントを別々にレポートすることに注意してください。詳細については、スタック構成のデバイスの管理（4-47 ページ）を参照してください。

セキュリティ コンテキスト（Security Context）

トラフィックが通過した仮想ファイアウォール グループを特定するセキュリティ コンテキストの名前を入力します。システムがこのフィールドにデータを設定するのは、マルチ コンテキスト モードの ASA FirePOWER デバイスだけです。

インターフェイス（入力、出力）（Interface（Ingress、Egress））

イベントをトリガーしたパケットと関連付けられたインターフェイスの名前を入力します。センシング インターフェイスの設定（4-66 ページ）を参照してください。

侵入ポリシー（Intrusion Policy）

イベントと関連付けられた侵入ポリシー名を入力します。侵入ポリシーの管理（31-3 ページ）を参照してください。

アクセス コントロール ポリシー（Access Control Policy）

イベントと関連付けられたアクセス コントロール ポリシー名を入力します。アクセス コントロール ポリシーの管理（12-12 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（Access Control Rule）

イベントと関連付けられたアクセス コントロール ルールの名前を入力します。アクセス コントロール ルールを使用したトラフィック フローの調整（14-1 ページ）を参照してください。

HTTP ホスト名（HTTP Hostname）

HTTP 要求のホスト ヘッダーから取得された単一のホスト名を指定します。

ホスト名を HTTP クライアント トラフィックの侵入イベントと関連付けるには、HTTP 検査プリプロセッサの [ホスト名の記録（Log Hostname）] オプションを有効にする必要があります。詳細については、サーバレベル HTTP 正規化オプションの選択（27-36 ページ）を参照してください。

HTTP URI

侵入イベントをトリガーした HTTP 要求パケットと関連付けられた単一 URI を指定します。

URI を HTTP トラフィックの侵入イベントと関連付けるには、HTTP 検査プリプロセッサの [URI の記録（Log URI）] オプションを有効にする必要があります。詳細については、サーバレベル HTTP 正規化オプションの選択（27-36 ページ）を参照してください。

メール送信者（Email Sender）

SMTP MAIL FROM コマンドから取得された電子メール送信者のアドレスを指定します。また、カンマ区切りリストを入力して、すべての指定アドレスに関連付けられているイベントを検索することもできます。詳細については、侵入イベントについて（41-12 ページ）を参照してください。

電子メール受信者（Email Recipient）

SMTP RCPT TO コマンドから取得された電子メール受信者のアドレスを指定します。また、カンマ区切りリストを入力して、すべての指定アドレスに関連付けられているイベントを検索することもできます。詳細については、侵入イベントについて（41-12 ページ）を参照してください。

電子メール添付ファイル（Email Attachments）

MIME Content-Disposition ヘッダーから取得された MIME 添付ファイル名を指定します。リスト内のすべての添付ファイル名に関連付けられているイベントを検索するには、カンマ区切りリストを入力します。詳細については、侵入イベントについて（41-12 ページ）を参照してください。

電子メールのヘッダー（Email Headers）

電子メール ヘッダーから取得したデータを指定します。電子メール ヘッダーは侵入イベントのテーブル ビューには表示されませんが、電子メール ヘッダー データは検索条件として使用できることに注意してください。

電子メール ヘッダーを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [ヘッダーの記録（Log Headers）] オプションを有効にする必要があります。詳細については、SMTP デコードについて（27-65 ページ）を参照してください。

確認者（Reviewed By）

イベントを確認したユーザの名前を指定します。侵入イベントの確認（41-18 ページ）を参照してください。

ヒント　unreviewed と入力すると、まだ確認されていないイベントを検索できます。

侵入イベントの特別な検索構文

前述の一般的な検索構文の補足として、以下で侵入イベントの特別な検索構文について説明します。

実行された実際の SSL アクション（The SSL Actual Action taken）

指定したアクションが適用された暗号化トラフィックに対する侵入イベントを表示するには、次のいずれかのキーワードを入力します。

- [復号しない（Do not Decrypt）] は、システムが復号しなかった接続を表します。
- [ブロック（Block）] および [リセットしてブロック（Block with Reset）] は、ブロックされた暗号化接続を表します。
- [復号（既知のキー）（Decrypt (Known Key)）] は、既知の秘密キーを使用して復号された着信接続を表します。
- [復号（キーの置き換え）（Decrypt (Replace Key)）] は、置き換えられた公開キーと自己署名サーバ証明書を使用して復号された発信接続を表します。
- [復号（再署名）（Decrypt (Resign)）] は、再署名サーバ証明書を使用して復号された発信接続を表します。

この列は、侵入イベント テーブル ビューには表示されません。

SSL 障害の理由（The SSL Failure Reason）

指定した理由で、復号に失敗した暗号化トラフィックに対する侵入イベントを表示するには、次のいずれかのキーワードを入力します。

- 不明
- 不一致（No Match）
- Success
- キャッシュされないセッション（Uncached Session）
- 不明な暗号スイート（Unknown Cipher Suite）
- サポートされていない暗号スイート（Unsupported Cipher Suite）
- サポートされていない SSL バージョン（Unsupported SSL Version）
- SSL 圧縮の使用（SSL Compression Used）
- パッシブ モードで復号できないセッション（Session Undecryptable in Passive Mode）
- ハンドシェイク エラー（Handshake Error）
- 復号化エラー（Decryption Error）
- 保留サーバ名カテゴリ ルックアップ（Pending Server Name Category Lookup）
- 保留共通名カテゴリ ルックアップ（Pending Common Name Category Lookup）
- 内部エラー（Internal Error）
- ネットワーク パラメータを使用できません（Network Parameters Unavailable）
- 無効なサーバ証明書の処理（Invalid Server Certificate Handle）
- サーバ証明書フィンガープリントを使用できません（Server Certificate Fingerprint Unavailable）

- サブジェクト DN をキャッシュできません(Cannot Cache Subject DN)
- 発行元 DN をキャッシュできません(Cannot Cache Issuer DN)
- 不明の SSL バージョン(Unknown SSL Version)
- 外部証明書リストを使用できません(External Certificate List Unavailable)
- 外部証明書フィンガープリントを使用できません(External Certificate Fingerprint Unavailable)
- 内部証明書リストが無効です(Internal Certificate List Invalid)
- 内部証明書リストを使用できません(Internal Certificate List Unavailable)
- 内部証明書を使用できません(Internal Certificate Unavailable)
- 内部証明書フィンガープリントを使用できません(Internal Certificate Fingerprint Unavailable)
- サーバ証明書検証を使用できません(Server Certificate Fingerprint Unavailable)
- サーバ証明書検証エラー(Server Certificate Validation Failure)
- Invalid Action

この列は、侵入イベント テーブル ビューには表示されません。

SSL 対象国(The SSL Subject Country)

証明書の対象国に関連付けられている暗号化トラフィックに対する侵入イベントを表示するには、2 文字の ISO 3166-1 alpha-2 国コードを入力します。

この列は、侵入イベント テーブル ビューには表示されません。

SSL 発行国(The SSL Issuer Country)

証明書の発行国に関連付けられている暗号化トラフィックに対する侵入イベントを表示するには、2 文字の ISO 3166-1 alpha-2 国コードを入力します。

この列は、侵入イベント テーブル ビューには表示されません。

SSL 証明書のフィンガープリント(SSL Certificate Fingerprint)

証明書に関連付けられているトラフィックに対する侵入イベントを表示するには、証明書の認証に使用された SHA ハッシュ値を入力するか、貼り付けます。

この列は、侵入イベント テーブル ビューには表示されません。

SSL 公開キーのフィンガープリント(SSL Public Key Fingerprint)

証明書に関連付けられているトラフィックに対する侵入イベントを表示するには、証明書に含まれている公開キーの認証に使用された SHA ハッシュ値を入力するか、貼り付けます。

この列は、侵入イベント テーブル ビューには表示されません。

侵入イベントを検索する方法:

アクセス: Admin/Intrusion Admin

手順 1　[分析(Analysis)] > [検索(Search)] を選択します。

[侵入イベント(Intrusion Events)] 検索ページが表示されます。

侵入イベントのリストを表示しているときに([分析(Analysis)] > [侵入(Intrusions)] > [イベント(Events)])、[検索(Search)] をクリックすることもできます。

手順 2　手順の上の表に示されているように、該当するフィールドに検索条件を入力します。

- 検索でのオブジェクトの使用を含む検索構文の詳細については、イベントの検索（60-1 ページ）を参照してください。
- 公開キー証明書に関連するフィールドについては、暗号化接続に関連付けられた証明書の表示（39-34 ページ）を参照してください。
- 侵入イベントの特別な検索構文については、侵入イベントの特別な検索構文（41-52 ページ）を参照してください。

手順 3　必要に応じて検索を保存する場合は、[プライベート（Private）] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　カスタム ユーザ ロールのデータの制限として検索を使用する場合は、必ずプライベート検索として保存する**必要**があります。

手順 4　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [保存（Save）] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存（Save）] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[プライベート（Private）] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[新規として保存（Save As New）] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存（Save）] をクリックします。検索が保存され（[プライベート（Private）] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

手順 5　検索を開始するには、[検索（Search）] ボタンをクリックします。

検索結果は、現在の時刻範囲によって制約される、デフォルトの侵入イベント ワークフローに表示されます。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

クリップボードの使用

ライセンス：Protection

クリップボードは、任意の侵入イベント ビューから侵入イベントをコピーできる保存エリアです。クリップボードにイベントを追加する方法については、ドリルダウン ページとテーブル ビュー ページの使用（41-21 ページ）およびパケット ビューの使用（41-25 ページ）を参照してください。

クリップボードの内容は、イベントが生成された日時別にソートされます。クリップボードに侵入イベントを追加した後、クリップボードからそれらを削除することも、クリップボードの内容のレポートを生成することもできます。

クリップボードの侵入イベントをインシデントに追加することもできます。インシデントとは、セキュリティ ポリシーの違反の可能性に関係していると思われるイベントのコンパイルです。クリップボードからインシデントにイベントを追加する方法の詳細については、インシデントの作成（42-5 ページ）を参照してください。

詳細については、次の各項を参照してください。

- クリップボードのレポートの生成（41-55 ページ）
- クリップボードからのイベントの削除（41-56 ページ）

クリップボードのレポートの生成

ライセンス：Protection

任意のイベント ビューで行うのと同じように、クリップボードのイベントに関するレポートを生成できます。

クリップボードの侵入イベントのレポートを生成する方法：

アクセス：Admin/Intrusion Admin

手順 1　次のように、クリップボードに 1 つ以上のイベントを追加します。

- ドリルダウン ページまたはイベントのテーブル ビューからクリップボードにイベントを追加する方法については、ドリルダウン ページとテーブル ビュー ページの使用（41-21 ページ）を参照してください。
- パケット ビューからクリップボードにイベントを追加する方法については、パケット ビューの使用（41-25 ページ）を参照してください。

手順 2　[分析（Analysis）] > [侵入（Intrusions）] > [クリップボード（Clipboard）] を選択します。

クリップボードが表示されます。

手順 3　次の選択肢があります。

- クリップボード上のページの特定のイベントを含めるには、そのページに移動し、イベントの横にあるチェックボックスを選択し、[レポートの生成（Generate Report）] をクリックします。
- クリップボードのすべてのイベントを含めるには、[すべてのレポートを生成（Generate Report All）] をクリックします。

いずれの場合も、[レポート テンプレート（Report Templates）] ページが表示されます。

手順 4　レポートの表示方法を指定してから、[生成（Generate）] をクリックします。

[レポートの生成（Generate Report）] ポップアップ ダイアログが表示されます。

手順 5　1 つ以上の出力形式（HTML、PDF、CSV）を選択し、オプションで、他の設定を変更します。

ヒント　レポート デザイナの使用方法の詳細については、レポートの操作（57-1 ページ）を参照してください。

手順 6　[生成（Generate）] をクリックし、[はい（Yes）] をクリックします。

[レポート生成完了（Report Generation Complete）] ポップアップ ウィンドウと、レポートを表示するためのリンクが表示されます。

手順 7　次のいずれかをクリックします。

- レポートのリンク。新しいウィンドウが開き、選択したレポートが表示されます。
- [OK]。レポートのデザインを変更できる [レポート テンプレート（Report Templates）] ページに戻ります。

クリップボードからのイベントの削除

ライセンス：Protection

インシデントに追加したくない侵入イベントがクリップボード上に存在する場合は、そのイベントを削除できます。

（注） クリップボードからイベントを削除しても、イベント データベースからイベントは削除**されません**。ただし、イベント データベースからイベントを削除すると、イベントはクリップボードから削除されます。

イベントをクリップボードから削除する方法：

アクセス：Admin/Intrusion Admin

手順 1　[分析（Analysis）] > [侵入（Intrusions）] > [クリップボード（Clipboard）] を選択します。

クリップボードが表示されます。

手順 2　次の選択肢があります。

- クリップボード上のページの特定の侵入イベントを削除するには、そのページに移動し、イベントの横にあるチェックボックスを選択し、[削除（Delete）] をクリックします。

  イベントが削除されます。

- クリップボードのすべての侵入イベントを削除するには、[すべて削除（Delete All）] をクリックします。

  すべてのイベントがクリップボードから削除されます。[イベント設定（Event Preferences）] で [すべてのアクションの確認（Confirm 'All' Actions）] オプションを選択した場合、最初にすべてのイベントを削除するかどうか確認するプロンプトが表示されることに注意してください。