



## 侵入イベントの操作

以下のトピックでは、侵入イベントを操作する方法について説明します。

- [侵入イベントについて \(1 ページ\)](#)
- [侵入イベントの表示 \(2 ページ\)](#)
- [侵入イベントのワークフロー ページ \(23 ページ\)](#)
- [侵入イベントのクリップボード \(46 ページ\)](#)
- [侵入イベントの統計情報の表示 \(48 ページ\)](#)
- [侵入イベントのパフォーマンス グラフの表示 \(50 ページ\)](#)
- [侵入イベント グラフの表示 \(57 ページ\)](#)
- [侵入イベントの履歴 \(58 ページ\)](#)

## 侵入イベントについて

Firepower 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（古い用語で「IPS イベント」と呼ばれることもあります）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データです。パケットベースのイベントの場合、イベントをトリガーとして使用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、Firepower Management Center 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的確に把握できます。

管理対象デバイスをインライン、スイッチド、またはルーテッド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。

## 侵入イベントの表示

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

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。

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と、イベントビューの表示が遅くなる場合があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

**ステップ1** [Analysis] > [Intrusions] > [Events]を選択します。

**ステップ2** 次の選択肢があります。

- 時間範囲の調整：時間枠の変更の説明に従って、イベントビューの時間範囲を調整します。
- ワークフローの変更：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、システム提供のワークフローのいずれかを選択します。
- 制約：表示する対象を分析において重要な侵入イベントに狭めるには、[侵入イベントワークフローの使用 \(24 ページ\)](#) を参照してください。
- イベントの削除：データベースからイベントを削除するには、[削除 (Delete)] をクリックして表示しているパケットのイベントを削除するか、[すべて削除 (Delete All)] をクリックして以前に選択したパケットのすべてのイベントを削除します。
- 確認済みのマークを付ける：侵入イベントに確認済みのマークを付けるには、[侵入イベントを確認済みとしてマーク \(18 ページ\)](#) を参照してください。
- 接続データの表示：侵入イベントに関連付けられた接続データを表示するには、[侵入イベントと関連付けられた接続データの表示 \(17 ページ\)](#) を参照してください。
- 内容の表示：[侵入イベント フィールド \(3 ページ\)](#) の説明に従ってテーブルのカラムの内容を表示します。

### 関連トピック

[侵入イベント パケット ビューの使用 \(28 ページ\)](#)

## 侵入イベントのフィールドについて

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データです。パケットベースのイベントの場合、イベントをトリガーとして使用したパケットのコピーも記録されます。

侵入イベント データは [分析 (Analysis) ] ト> [侵入 (Intrusions) ]> [イベント (Events) ] で Firepower Management Center Web インターフェイスで表示できます。または外部ツールを使用して使用状況の syslog メッセージの特定のフィールドからデータをエミットします。Syslog のフィールドは下のリストに示されます。同等の syslog がリストされていないフィールドは、syslog メッセージでは使用可能できません。

侵入イベントを検索するときは、個別のイベントで利用可能な情報は、システムがいつ、なぜ、どのようにしてイベントを記録したかによって異なることに注意してください。たとえば、復号化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 TLS/SSL 情報を含んでいます。



- (注) Firepower Management Center の Web インターフェイスの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ます。セッション中にフィールドを有効にするには、検索制約を拡張してから、[無効の列 (Disabled Columns) ] の下の列名をクリックします。

## 侵入イベント フィールド

### [アクセス コントロール ポリシー (Access Control Policy) ] (syslog : ACPolicy)

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に関連付けられているアクセス コントロール ポリシー。

### アクセス コントロール ルール

イベントを生成した侵入ルールを呼び出したアクセス コントロールルール。[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。

次の場合、このフィールドは空になります。

- [関連付けられたルールなし/デフォルトアクションなし (No associated rule/default action) ] : 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。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。

- [関連付けられている接続イベントなし (No associated connection event) ] : セッションに記録された接続イベントがデータベースから消去されている場合。たとえば、接続イベントに侵入イベントよりも高いターンオーバーがある場合などです。

#### [アプリケーション プロトコル (Application Protocol) ] (syslog : ApplicationProtocol)

(使用可能な場合) 侵入イベントをトリガーとして使用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。

#### アプリケーション プロトコル カテゴリとタグ (Application Protocol Category and Tag)

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。

#### [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ているリスク。[非常に高い (Very High) ]、[高 (High) ]、[中 (Medium) ]、[低 (Low) ]、および [非常に低い (Very Low) ]。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。

#### 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ているビジネスとの関連性。[非常に高い (Very High) ]、[高 (High) ]、[中 (Medium) ]、[低 (Low) ]、および [非常に低い (Very Low) ]。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。

#### [分類 (Classification) ] (syslog : Classification)

イベントを生成したルールが属する分類。

[侵入イベント詳細](#)で、使用可能な分類値のリストを参照してください。

このフィールドを検索するときは、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。また、番号、名前、または説明のカンマ区切りリストを入力することもできます。最後に、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。

#### [クライアント (Client) ] (syslog : Client)

(使用可能な場合) 侵入イベントをトリガーとして使用したトラフィックで検出されたモニター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。

#### クライアント カテゴリとタグ (Client Category and Tag)

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。

**(Syslog のみ)**

ある接続と別の同時接続を区別するカウンタ。このフィールドは、それ自体には意味がありません。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを一意に識別できます。

**(Syslog のみ)**

接続イベントを処理した Snort インスタンス。このフィールドは、それ自体には意味がありません。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを一意に識別できます。

**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。このフィールドは検索できません。

**CVE ID**

このフィールドは検索フィールド専用です。

MITRE の Common Vulnerabilities and Exposures (CVE) データベース (<https://cve.mitre.org/>) の脆弱性に関連付けられた識別番号による検索。

**送信先の大陸 (Destination Continent)**

侵入イベントに関連する受信ホストの大陸。

**送信先の国 (Destination Country)**

侵入イベントに関連する受信ホストの国。

**[宛先IP (Destination IP) ] (syslog : DstIP)**

侵入イベントに関連する受信ホストが使用する IP アドレス。

**[宛先ポート/ICMPコード (Destination Port/ICMP Code) ] (syslog : DstPort、ICMPCode)**

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、このフィールドには ICMP コードが表示されます。

**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。

## Device

アクセス コントロール ポリシーが展開された管理対象デバイス。

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、別々のデバイスであるかのように侵入イベントをレポートすることに注意してください。

## ドメイン (Domain)

侵入を検出したデバイスのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

## [出力インターフェイス (Egress Interface) ] (syslog : EgressInterface)

イベントをトリガーとして使用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。

## [出力セキュリティ ゾーン (Egress Security Zone) ] : (syslog : EgressZone)

イベントをトリガーとして使用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。

## 電子メールの添付ファイル (Email Attachments)

MIME の Content-Disposition 見出しから取得された 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 [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。

## 電子メールのヘッダー (Email Headers)

このフィールドは検索フィールド専用です。

電子メールのヘッダーから取得したデータ。

電子メールのヘッダーを 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 [ヘッダーのログ (Log Headers) ] オプションを有効にする必要があります。

## メール受信者 (Email Recipient)

SMTPRCPTTO 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 [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。

## 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 [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。

**(Syslog のみ)**

システムが最初のパケットを検出した時間。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを一意に識別できます。

**ジェネレータ (Generator)**

イベントを生成したコンポーネント。

次の侵入イベントフィールドに関する情報も参照してください。[GID]、[メッセージ (Message)]、および [Snort ID]

**GID (syslog のみ)**

ジェネレータ ID。イベントを生成したコンポーネントの ID。

次の侵入イベントフィールドに関する情報も参照してください。[ジェネレータ (Generator)]、[メッセージ (Message)]、および [Snort ID]

**HTTP ホスト名 (HTTP Hostname)**

HTTP 要求のホスト見出し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 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 [ホスト名のログ (Log Headers)] オプションを有効にする必要があります。

テーブル ビューで、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。

**[HTTP 応答コード (HTTP Response Code)] (syslog : HTTPResponse)**

イベントをトリガーした接続を介してクライアントの HTTP 要求に応答して送信される HTTP ステータス コード。

**HTTP URI**

(存在する場合) 侵入イベントをトリガーとして使用した 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。

URI 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 [URI のログ (Log URI)] オプションを有効にする必要があります。

HTTP 応答によってトリガーとして使用された侵入イベントの関連 HTTP URI を参照するには、[両方のポートでのストリーム再構成の実行 (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。

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。

### 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。

このフィールドを検索するときは、影響アイコンの色または一部の文字列を指定しないでください。たとえば、**blue**、**level 1**、または **0** を使用しないでください。有効な大文字と小文字を区別しない値は次のとおりです。

- Impact 0、Impact Level 0
- Impact 1、Impact Level 1
- Impact 2、Impact Level 2
- Impact 3、Impact Level 3
- Impact 4、Impact Level 4

NetFlow データからネットワーク マップに追加されたホストに使用可能なオペレーティングシステムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクトレベル1：赤）インパクトレベルを割り当てることができません。このような場合は、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 ID を手動で設定します。

### 入力インターフェイス (Syslog : IngressInterface)

イベントをトリガーとして使用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。

### [入力セキュリティゾーン (Ingress Security Zone)] : (syslog : IngressZone)

イベントをトリガーとして使用したパケットの入力セキュリティゾーンまたはトンネルゾーン。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。

### [インライン結果 (Inline Result)] (syslog : InlineResult)

ワークフローとテーブルビューでは、このフィールドには次のいずれかが表示されます。

表 1: ワークフロービューとテーブルビューの [インライン結果 (Inline Result)] フィールドの内容

アイコン	意味
黒の下矢印	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ました



アイコン	意味
グレーの下矢印	[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、またはシステムがブ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
アイコンなし (空白)	トリガーされたルールは [ドロップしてイベントを生成する (Drop and Generate Events) ] に設定されていませんでした

パッシブ展開では、侵入ポリシーのルールの状態やインラインドロップ動作に関係なく、インラインインターフェイスがタップモードの場合を含めて、システムはパケットをドロップしません。

このフィールドを検索するときは、次のいずれかを入力します。

- **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 (Intrusion Policy) ] (syslog : IntrusionPolicy)**

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。

**IOC (syslog : NumIOC)**

侵入イベントをトリガーとして使用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痕跡 (IOC) もトリガーとして使用したかどうか。

このフィールドを検索するときは、**triggered** または **n/a** を指定します。

**[メッセージ (Message) ] (syslog : 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。

ジェネレータおよび Snort ID (GID と SID) と SID バージョン (改訂) はカッコで囲んだコロン区切りの数字形式で各メッセージの末尾に付加されます (GID:SID:version)。例 :

**(1:36330:2)**。

**[MPLS ラベル (MPLS Label) ] (syslog : MPLS\_Label)**

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。

**[ネットワーク分析ポリシー (Network Analysis Policy) ] (syslog : NAPPolicy)**

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 (ある場合)。

このフィールドには、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。

**クライアントのオリジナル 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、ネットワーク解析ポリシーで HTTP プリプロセッサ [元のクライアント 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、ネットワーク解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 見出しを指定し、システムが [クライアントのオリジナル IP (Original Client IP) ] イベント フィールドの値を選択する優先順位を設定します。

**[優先度 (Priority) ] (syslog : Priority)**

Cisco Talos Intelligence Group (Talos) で指定されたイベントの優先度。優先度は、`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。

**[プロトコル (Protocol) ] (syslog : Protocol)**

Firepower Management Center の Web インターフェイスでは、このフィールドは検索フィールド専用です。

<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。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。

**確認者 (Reviewed By)**

イベントを確認したユーザの名前。このフィールドを検索するときは、**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。

**Revision (syslog のみ)**

イベントの生成に使用された署名のバージョン。

次の侵入イベントフィールドに関する情報も参照してください。[ジェネレータ (Generator) ]、[GID]、[メッセージ (Message) ]、[SID]、および [Snort ID]

**[セキュリティ コンテキスト (Security Context) ] (syslog : 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 だけです。

**(Syslog のみ)**

イベントを生成した Firepower デバイスの一意の識別子。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを一意に識別できます。

**SID (syslog のみ)**

イベントを生成したルールの署名 ID (Snort ID ともいう)

次の侵入イベントフィールドに関する情報も参照してください。[ジェネレータ (Generator) ]、[GID]、[メッセージ (Message) ]、[改訂 (Revision) ]、および [Snort ID]

**Snort ID**

このフィールドは検索フィールド専用です。

(syslog フィールドについては、SID を参照してください。)

検索の実行時： イベントを生成したルールの [SnortID] (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 2 : [Snort ID] 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 のコンマ区切りリスト	10000,11000,12000
単一の GID:SID の組み合わせ	1:10000
GID:SID の組み合わせのコンマ区切りリスト	1:10000,1:11000,1:12000

値	例
SID および GID:SID の組み合わせのコマ区切りリスト	10000,1:11000,12000

表示しているイベントの SID が [メッセージ (Message)] 列に表示されます。詳細については、この項の [メッセージ (Message)] フィールドについての説明を参照してください。

**ソースの大陸 (Source Continent)**

侵入イベントに関連する送信ホストのある大陸。

**ソースの国 (Source Country)**

侵入イベントに関連する送信ホストのある国。

**[送信元 IP (Source IP)] (syslog : SrcIP)**

侵入イベントに関連する送信ホストが使用する IP アドレス。

**[送信元ポート/ICMP タイプ (Source Port/ICMP Type)] (syslog : SrcPort、ICMPType)**

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、このフィールドには ICMP タイプが表示されます。

**[送信元ユーザ (Source User)] (syslog : 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。

**SSL Actual Action (Syslog: SSLActualAction)**

In the Firepower Management Center web interface, this field is a search field only.

システムが暗号化されたトラフィックに適用したアクション。

**[ブロック (Block) /リセットしてブロック (Block With Reset)]**

ブロックされた暗号化接続を表します。

**[復号 (再署名) (Decrypt (Resign))]**

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 (キーの交換) (Decrypt (Replace Key))]**

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化された発信接続を表します。

**[復号 (既知のキー) (Decrypt (Known Key))]**

既知の秘密キーを使用して復号化された着信接続を表します。

**[デフォルトアクション (Default Action)]**

接続がデフォルトアクションによって処理されたことを示します。

**[復号しない (Do not Decrypt) ]**

システムが復号化しなかった接続を表します。

フィールド値は、検索ワークフロー ページの [SSL ステータス (SSL Status) ] フィールドに表示されます。

**[SSL 証明書情報 (SSL Certificate Information) ]**

このフィールドは検索フィールド専用です。

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- サブジェクト/発行元共通名 (Subject/Issuer Common Name)
- サブジェクト/発行元組織 (Subject/Issuer Organization)
- サブジェクト/発行元組織単位 (Subject/Issuer Organization Unit)
- 有効期間 (Not Valid Before/After)
- シリアル番号 (Serial Number)
- 証明書フィンガープリント (Certificate Fingerprint)
- 公開キー フィンガープリント (Public Key Fingerprint)

**SSL 失敗理由 (SSL Failure Reason)**

このフィールドは検索フィールド専用です。

システムが暗号化されたトラフィックの復号化に失敗した理由。

- 不明
- No Match
- Success
- Uncached Session
- 不明な暗号スイート
- サポートされていない暗号スイート
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup

- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- 無効なアクション (Invalid Action)

フィールド値は、検索ワークフローのページの [SSL ステータス (SSL Status) ] フィールドに表示されます。

### SSL ステータス (SSL Status)

暗号化接続をログに記録した [SSL の実際のアクション (SSL Actual Action) ] (SSL ルール、デフォルトのアクション、または復号化できないトラフィックアクション) に関連付けられているアクション。

システムが暗号化接続を復号できなかった場合は、[SSL の実際の動作 (SSL Actual Action) ] (実行された復号不能のトラフィックアクション) と、[SSL 失敗理由 (SSL Failure Reason) ] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [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。

このフィールドを検索する場合は、[SSL の実際の動作 (SSL Actual Action) ] と [SSL 失敗理由 (SSL Failure Reason) ] の 1 つ以上の値を入力することで、システムが処理した、または復号に失敗した暗号化トラフィックが表示されます。

### [SSL サブジェクト/発行元国 (SSL Subject/Issuer Country) ]

このフィールドは検索フィールド専用です。

暗号化証明書に関連付けられている件名または発行者の国に関する 2 文字の ISO 3166-1 アルファ 2 国コード。

#### 時刻 (Time)

イベントの日付と時刻。このフィールドは検索できません。

#### [VLAN ID] (syslog : VLAN\_ID)

侵入イベントをトリガーとして使用したパケットと関連付けられた最内部 VLAN ID。

#### [Web アプリケーション (Web Application) ] (syslog : WebApplication)

侵入イベントをトリガーとして使用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、特定の Web アプリケーションを検出できなかった場合、システムは代わりに一般的な Web ブラウジング指定を提供します。

#### Web アプリケーションのカテゴリとタグ (Web Application Category and Tag)

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。

#### 関連トピック

[イベントの検索](#)

## 侵入イベント影響レベル

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、Firepower Management Center 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、システム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、脆弱性情報との関係を色で示します。



- (注) NetFlow データからネットワークマップに追加されたホストに使用可能なオペレーティングシステムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な (インパクトレベル 1 : 赤) インパクトレベルを割り当てることができません。このような場合は、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 ID を手動で設定します。

次の表に、影響レベルで使用可能な値を示します。

表 3: 影響レベル

影響レベル	脆弱性	色	説明
0	Unknown	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	レッド	次のいずれかを行います。 <ul style="list-style-type: none"> <li>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</li> <li>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。</li> </ul>
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。 <ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul>



影響レベル	脆弱性	色	説明
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。 <ul style="list-style-type: none"> <li>ポート指向のトラフィック（たとえば、TCP または UDP）の場合、ポートが開いていません</li> <li>ポート指向ではないトラフィック（たとえば、ICMP）の場合、ホストはプロトコルを使用しません</li> </ul>
4	不明なターゲット	ブルー	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。

## 侵入イベントと関連付けられた接続データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

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。

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。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

**ステップ 1** [Analysis] > [Intrusions] > [Events] を選択します。

**ステップ 2** テーブル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、[ジャンプ (Jump to)] ドロップダウン リストから [接続 (Connections)] を選択します。

ヒント 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ション](#)」を参照してください。

#### 関連トピック

[許可された接続のロギング](#)

[侵入イベント ワークフローの使用](#) (24 ページ)

[接続およびセキュリティ インテリジェンス イベント テーブルの使用](#)

## 侵入イベントを確認済みとしてマーク

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

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。

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（たとえば、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ているなど）、そのイベントを確認済みとしてマークできます。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、デフォルトの侵入イベントページには表示されなくなります。自分の名前がレビューアとして表示されます。

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

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。こうして復元された侵入イベントは、[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。

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オンにして、[レビュー (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。

#### 関連トピック

[侵入イベント ワークフローの使用](#) (24 ページ)

## 以前に確認された侵入イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

**ステップ 1** [Analysis] > [Intrusions] > [Reviewed Events] を選択します。

**ステップ 2** 次の選択肢があります。

- [時間枠の変更](#)の説明に従って、時間範囲を調整します。
- 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、システム提供のワークフローのいずれかを選択します。
- 表示されるイベントの詳細については、[侵入イベント フィールド \(3 ページ\)](#) を参照してください。

### 関連トピック

[侵入イベント ワークフローの使用 \(24 ページ\)](#)

## 侵入イベントへの未確認としてマーク

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

イベントに未確認のマークを付けることで、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。

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

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、特定のイベントの横にあるチェックボックスをオンにして、[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。

## プリプロセッサ イベント

プリプロセッサが提供する機能は2つあります。1つは、パケットに対して指定されたアクション（HTTP トラフィックを復号して正規化するなど）を実行する機能、もう1つは、パケットが特定のプリプロセッサ オプションをトリガーしたときに関連するプリプロセッサ ルールが有効にされている場合は常にイベントを生成することで、指定のプリプロセッサ オプションの実行を報告するという機能です。たとえば、プリプロセッサが IIS の二重にエンコードされたトラフィックを検出した場合にイベントが生成されるようにするには、HTTP Inspect の [二重エンコード (Double Encoding)] オプションと、HTTP Inspect Generator (GID) 119 および [Snort ID] (SID) 2 が設定された関連するプリプロセッサ ルールを有効にします。

プリプロセッサの実行を報告するイベントを生成すると、異常なプロトコルエクスプロイトを検出するのに役立ちます。たとえば、攻撃者は、ホスト上で DoS 攻撃を引き起こす重複 IP フラグメントを細工することがあります。IP 最適化プリプロセッサはこの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。

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表示されないという点で、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、GID、SID、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であるかをどうか判断して、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、その結果に応じ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報告します。

## プリプロセッサのジェネレータ ID

各プリプロセッサには、独自のジェネレータ ID 番号 (GID) があり、これはパケットによってトリガーとして使用されたプリプロセッサを示します。一部のプリプロセッサは関連した SID もあり、これは潜在的攻撃を分類する ID 番号です。ルールの ([Snort ID]SID) が、ルールをトリガーとして使用するパケットのコンテキストを提供できる方法とほぼ同じで、この ID 番号によりイベントのタイプを分類することによって、イベントをより効率的に分析するのに役立ちます。侵入ポリシー ルールのページのプリプロセッサ フィルター グループのプリプロセッサごとにプリプロセッサルールをリストできます。また、プリプロセッサのプリプロセッサルールとカテゴリ フィルター グループのパケット デコーダ サブグループをリストできます。



(注) 標準テキストルールによって生成されるイベントは、ジェネレータ ID が 1 (グローバルドメインまたはレガシー GID) または 1000 ~ 2000 (子孫ドメイン) です。共有オブジェクトルールの場合、イベントのジェネレータ ID は 3 です。どちらの場合も、トリガーした特定のルールがイベントの SID に示されます。

次の表では、各 GID を生成するイベントのタイプについて説明します。

表 4: ジェネレータ ID

ID	コンポーネント	説明
1	標準的なテキストルール	パケットが標準テキストルールをトリガーとして使用したときにイベントが生成されました (グローバルドメインまたはレガシー GID)。
2	タグ付きパケット	タグ付きセッションからパケットを生成するタグジェネレータによって、イベントが生成されました。これは、tag ルールオプションが使用される場合に発生します。
3	共有オブジェクトルール	パケットが共有オブジェクトルールをトリガーとして使用したときにイベントが生成されました。
102	HTTP デコーダ	デコーダエンジンが、パケット内の HTTP データを復号化しました。
105	Back Orifice ディテクタ	Back Orifice ディテクタが、パケットに関連付けられた Back Orifice 攻撃を特定しました。
106	RPC デコーダ	RPC デコーダがパケットを復号化しました。
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。
119、120	HTTP Inspect プリプロセッサ	HTTP Inspect プリプロセッサによってイベントが生成されました。GID 120 ルールは、サーバ固有の HTTP トラフィックに関するルールです。
122	ポートスキャン ディテクタ	ポートスキャンフロー ディテクタによってイベントが生成されました。

ID	コンポーネント	説明
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つたときに、イベントが生成されました。
124	SMTP デコーダ	SMTP プリプロセッサが SMTP バージ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。
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。
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。
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。
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。
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。
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。
134	ルール遅延 パケット遅延	ルール遅延によって侵入ルールのグループが中断された (134:1) または再有効化された (134:2) とき、あるいはパケット遅延しきい値が超過したために、システムがパケットの検査を停止したとき (134:3) に、イベントが生成されました。
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。
137	SSL プリプロセッサ	TLS/SSL プリプロセッサによってイベントが生成されました。

ID	コンポーネント	説明
138、139	機密データ プリプロセッサ	機密データプリプロセッサによってイベントが生成されました。
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。
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。
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。
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。
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。
145	DNP3 プリプロセッサ	DNP3 SCADA プリプロセッサによってイベントが生成されました。
1000～2000	標準的なテキストルール	パケットが標準テキストルールをトリガーとして使用したときにイベントが生成されました (子孫ドメイン)。

## 侵入イベントのワークフロー ページ

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。

Firepower 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2つ以上の列が含まれます。

「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減らすことができます。

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、発信元 IP アドレスおよびポート、宛先 IP アドレスおよびポート、イベントの優先度、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 [Time] をクリアすると、[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、[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、ルールをトリガーとして使用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として使用されるため、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。

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。

## 侵入イベントワークフローの使用

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

イベントのドリルダウンビューとテーブルビューは、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に分析を集中するために使用できる共通機能を共有します。



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。




**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。

**ステップ 1** [Analysis] > [Intrusions] > [Events] を使用して侵入イベントワークフローにアクセスします。

**ステップ 2** オプションで、[侵入イベントドリルダウンページの制約 \(27 ページ\)](#) または [侵入イベントテーブルビューの制約 \(28 ページ\)](#) の説明に従って、イベントビューに表示される侵入イベントの数を制限します。

**ステップ 3** 次の選択肢があります。

- 表示されるカラムの詳細については、[侵入イベントフィールド \(3 ページ\)](#) を参照してください。
- ホストのプロファイルを表示するには、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を表示するには、[送信元の国 (Source Country)] または [宛先の国 (Destination Country)] カラムに表示されるフラグアイコンをクリックします。
- (所属する組織でイベントデータを外部の Firepower システムに保存している場合) パケットや履歴データなど、イベントに関連する情報を調査するには、イベントの値を右クリックします。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、[を使用したイベント調査 Cisco Security Packet Analyzer](#) および [Web ベースのリソースを使用したイベントの調査](#) を参照してください。
- イベントに関する一般的なインテリジェンスを収集するには、テーブルでイベントの値を右クリックして、シスコまたはサードパーティのインテリジェンスソースを選択します。たとえば、不審な IP アドレスに関する詳細情報を [Cisco Talos](#) から入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、[Web ベースのリソースを使用したイベントの調査](#) を参照してください。
- 表示されたイベントの時刻と日付の範囲を変更するには、[時間枠の変更](#) 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、指定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。古い時間範囲を指定した場合、その時間範囲内のイベントが削除されることがあります。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。

(注) 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ます。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。

- 現在のワークフローページのイベントをソートする、または現在のワークフローページ内で移動するには、[ワークフローの使用](#)を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフローページの左上にある該当するページリンクをクリックします。
- 後でインシデントにイベントを転送できるように、クリップボードにイベントを追加するには、[コピー (Copy)] または [すべてコピー (Copy All)] をクリックします。
- イベントデータベースから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オンにし、[削除 (Delete)] または [すべて削除 (Delete All)] をクリックします。
- 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ようにするには、[侵入イベントを確認済みとしてマーク \(18 ページ\)](#) を参照してください。
- 選択したイベントをトリガーしたパケットのローカルコピー (libpcap 形式のパケットキャプチャファイル) 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オンにして、[パケットのダウンロード (Download Packets)] または [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には、[ワークフロー間のナビゲーション](#)を参照してください。
- 別のワークフローを一時的に使用するには、[(ワークフローの切り替え) ((switch workflow))] をクリックします。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク (Bookmark This Page)] をクリックします。
- [サマリーダッシュボード (Summary Dashboard)] の [侵入イベント (Intrusion Events)] セクションを表示するには、[ダッシュボード (Dashboards)] をクリックします。
- ブックマークの管理ページに移動するには、[ブックマークの表示 (View Bookmarks)] をクリックします。
- 現在のビューのデータに基づいてレポートを生成するには、[イベントビューからのレポートテンプレートの作成](#)を参照してください。

---

## 関連トピック

[イベントの検索](#)

[ブックマーク](#)

## 侵入イベント ドリルダウン ページの制約

次の表では、ドリルダウン ページの使用方法について説明します。

表 5: 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	<p>値をクリックします。</p> <p>たとえば、[Destination Port (宛先ポート)] ワークフローで、イベントを宛先がポート 80 であるものに制約するには、[DST Port/ICMP Code] 列で [80/tcp] をクリックします。ワークフローの次のページ [Events] が表示され、ポート 80/tcp のイベントだけが含まれます。</p>
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	<p>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、[View] をクリックします。</p> <p>たとえば、[Destination Port (宛先ポート)] 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、[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。</p> <p>複数の行を制約し、テーブルに複数の列が存在する場合 ([数 (Count)] 列を含まない) は、複合制約と呼ばれるものが作成されることに注意してください。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、[Event (イベント)] と [Destination (宛先)] の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くなります。</p>
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。

## 侵入イベント テーブル ビューの制約

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 6: イベントのテーブルビューでのイベントの制約

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 Port/ICMP Code] 列で [80/tcp] をクリックします。
テーブルから列を削除する	非表示にする列見出しのクローズアイコン (✕) 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。  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、該当するチェックボックスをオンまたはオフにします。無効になった列をビューに再追加するには、展開矢印 (▶) をクリックして検索制約を拡張し、[無効の列 (Disabled Columns)] の下の列名をクリックします。
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。 <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul>

## 侵入イベント パケット ビューの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

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として使用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、Firepower Management Center 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として使用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、優先度、イベントを生成したルール (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) 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として使用されるため、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。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

- ステップ 1** [侵入イベントテーブルビューの制約 \(28 ページ\)](#) の説明に従って、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。
- ステップ 2** 複数のイベントを選択した場合は、オプションで、ページの下部にあるページ番号を使用することによって、パケットビューでパケットのページを切り替えることができます。
- ステップ 3** 次のオプションもあります。
- 調整：パケットビューで日時範囲を変更するには、[時間枠の変更](#)を参照してください。
  - クリップボード：後でイベントをインシデントに転送するためクリップボードにそのイベントを追加するには、[コピー (Copy) ] をクリックして表示しているパケットのイベントをコピーするか、[すべてコピー (Copy All) ] をクリックして以前に選択したパケットのすべてのイベントをコピーします。
  - 設定：イベントをトリガした侵入ルールを設定するには、[アクション (Actions) ] の横にある矢印をクリックし、[パケットビュー内での侵入ルールの設定 \(34 ページ\)](#) の説明に従って操作を続けます。
  - 削除：データベースからイベントを削除するには、[削除 (Delete) ] をクリックして表示しているパケットのイベントを削除するか、[すべて削除 (Delete All) ] をクリックして以前に選択したパケットのすべてのイベントを削除します。
  - ダウンロード：イベントをトリガーしたパケットのローカルコピー (libpcap 形式のパケットキャプチャファイル) をダウンロードするには、[パケットのダウンロード (Download Packet) ] をクリックして表示しているイベントに関するキャプチャしたパケットのコピーを保存するか、[すべてのパケッ

トをダウンロード (Download All Packets) ] をクリックして以前に選択したパケットのすべてのイベントのキャプチャし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。

(注) 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ません。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。ダウンロードするには少なくとも 15% の使用可能なディスク領域が必要です。

- 確認済みのマークを付ける：イベントデータベースからは削除せずに、イベントビューから削除するため確認済みのイベントにマークを付けるには、[確認 (Review) ] をクリックして表示しているパケットのイベントにマークを付けるか、[すべて確認 (Review All) ] をクリックして以前に選択したパケットのすべてのイベントにマーク付けます。詳細については、[侵入イベントを確認済みとしてマーク \(18 ページ\)](#) を参照してください。
- 追加情報の表示：ページセクションを展開したり、折りたたんだりするには、セクションの横にある矢印をクリックします。詳細については、[イベント情報のフィールド \(30 ページ\)](#)、[フレーム情報のフィールド \(38 ページ\)](#)、[データリンク層情報フィールド \(39 ページ\)](#) を参照してください。
- ネットワーク層の情報の表示：[ネットワーク層情報の表示 \(40 ページ\)](#) を参照してください。
- パケットバイト情報の表示：[パケットバイト情報の表示 \(45 ページ\)](#) を参照してください。
- トランスポート層の情報の表示：次を参照してください。[トランスポート層情報の表示 \(42 ページ\)](#)

## 関連トピック

[ポートスキャン検出](#)

[侵入イベントのクリップボード \(46 ページ\)](#)

## イベント情報のフィールド

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。

### Event

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 ID です。Rev はルールのリビジョン番号です。

### Timestamp

パケットがキャプチャされた時刻 (UTC タイムゾーン)。

### 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。

### Priority

イベントの優先度。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。

### Ingress Security Zone

イベントをトリガーとして使用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。

### 出力セキュリティ ゾーン (Egress Security Zone)

イベントをトリガーとして使用したパケットの出力セキュリティゾーン。パッシブ展開では、このフィールドには入力されません。

### ドメイン (Domain)

管理対象デバイスが属するドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

### Device

アクセス コントロール ポリシーが展開された管理対象デバイス。

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、別々のデバイスであるかのように侵入イベントをレポートすることに注意してください。

### 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。マルチ コンテキストモードの ASA FirePOWER の場合に、システムがこのフィールドにデータを設定することに注意してください。

### 入力インターフェイス (Ingress Interface)

イベントをトリガーとして使用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。

### 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として使用したパケットの出力インターフェイス。

### 送信元/宛先 IP (Source/Destination IP)

イベントをトリガーとして使用したパケットの発生元（送信元）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として使用したトラフィックのターゲット（宛先）ホスト。

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

イベントをトリガーとして使用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。

### 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。

### Email Headers

電子メール 見出しから取得したデータ。電子メール 見出し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 見出し 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。

電子メールのヘッダーを 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 [ヘッダーのログ (Log Headers) ] オプションを有効にする必要があります。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 Hostname

（存在する場合）HTTP 要求のホスト 見出し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 1 行より長い場合は、完全なホスト名を展開できます。

ホスト名を表示するには、HTTP 検査プリプロセッサ [ホスト名のログ (Log Hostname) ] オプションを有効にする必要があります。

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として使用した 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 1 行より長い場合は、完全な URI を展開できます。

URI を表示するには、HTTP 検査プリプロセッサ [URI のログ (Log URI) ] オプションを有効にする必要があります。

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 が含まれる場合に表示されます。



HTTP 応答によってトリガーとして使用された侵入イベントの関連 HTTP URI を参照するには、[両方のポートでのストリーム再構成の実行 (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。

### 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。

### 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 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。[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。

### 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、管理者はユーザがローカルルールの表示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。

### アクション (Actions)

標準テキスト ルールとカスタム ルールのイベントの場合は、[アクション (Actions)] を展開して、イベントをトリガーとして使用したルールに次の操作のいずれかを実行します。

- ルールを編集する
- ルールのバージョンのドキュメントを表示します。標準的なテキストルールの場合、[アクション (Actions)] から [ドキュメントの表示 (View Documentation)] をクリックした後、ドキュメントのポップアップ ウィンドウの [ルール ドキュメント (Rule Documentation)] をクリックすると、より具体的なルールの詳細を表示することができます。
- 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

イベントが、共有オブジェクトルール、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 ビュー内での侵入ルールの設定

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

侵入イベントのパケットビュー内で、イベントをトリガーとして使用したルールに対して複数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。

**ステップ 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)] を展開します。

**ステップ 2** 次の選択肢があります。

- **コメント** : 標準テキストルール イベントの場合、[ルール 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、侵入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。
- **無効化** : [このルールを無効にする... (Disable this rule...)] をクリックして、ルールを無効にします。

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。

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、システム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。

- **パケットのドロップ** : [このルールを設定してトリガーパケットをドロップ... (Set this rule to drop the triggering packet...)] をクリックして、トリガーするパケットをドロップするルールを設定します。

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として使用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、システム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[インラインの場合ドロップ (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。

- **編集**：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編集します。イベントが、共有オブジェクトルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できません。

(注) システム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。

- **イベントの生成**：[このルールを設定してイベントを生成... (Set this rule to generate events...)] をクリックして、イベントを生成するルールを設定します。

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。

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、システムが提供するデフォルトポリシーは編集できません。

(注) 共有オブジェクトルールでパケットビューからイベントを生成したり、デフォルト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**。

- **抑制オプションの設定**：パケットビュー内での抑制オプションの設定 (37 ページ) の説明に従って、[抑制オプションの設定 (Set Suppression Options)] を展開し、続行します。

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、このイベントをトリガーとして使用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。

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の設定**：パケットビュー内でのしきい値オプションの設定 (36 ページ) の説明に従って、[しきい値オプションの設定 (Set Thresholding Options)] を展開し、続行します。

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も、これをトリガーとして使用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。

## パケットビュー内でのしきい値オプションの設定

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、システム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。

- ドキュメントの表示：[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の説明を確認します。次に、必要に応じて [ルールドキュメンテーション (Rule Documentation)] をクリックして、ルールの詳細を表示します。

## パケットビュー内でのしきい値オプションの設定

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

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。

**ステップ 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)] を展開します。

**ステップ 2** [しきい値オプションの設定 (Set Thresholding Options)] を展開し、次の 2 つの有効なオプションから 1 つを選択します。

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

(注) 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ます。たとえば、カスタムポリシーは編集できますが、システムが提供するデフォルトポリシーは編集できません。

**ステップ 3** 設定するしきい値のタイプを選択します。

- 通知を期間ごとに指定したイベントインスタンスの数の制限する場合は、[制限 (limit)] をクリックします。
- 期間ごとに指定したイベントインスタンス数に達するたびに通知を行う場合は、[しきい値 (threshold)] をクリックします。
- 指定されたイベントインスタンス数に達した後で、期間あたり 1 回ずつ通知を行う場合は、[両方 (Both)] をクリックします。

- ステップ4 該当するオプション ボタンをクリックして、イベント インスタンスを [送信元 (Source) ] IP アドレスと [宛先 (Destination) ] IP アドレスのどちらで追跡するかを指定します。
- ステップ5 [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。
- ステップ6 [秒 (Seconds) ] フィールドに、イベント インスタンスを追跡する期間を指定する数 (1 ~ 86400) を入力します。
- ステップ7 既存の侵入ポリシーでこのルール現在のしきい値をオーバーライドする場合は、[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) ] チェックボックスをオンにします。
- ステップ8 [しきい値の保存 (Save Thresholding) ] をクリックします。

パケットビュー内での抑制オプションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

抑制オプションを使用して、侵入イベントをまとめて、または送信元 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。

- ステップ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) ] を展開します。
- ステップ2 [抑制オプションの設定 (Set Suppression Options) ] を展開し、次の2つの有効なオプションから1つを選択します。

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

(注) 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ます。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。

- ステップ3 次のいずれかの [追跡対象 (Track By) ] オプションを選択します。
  - 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元 (Source) ] をクリックします。
  - 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先 (Destination) ] をクリックします。
  - 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場合は、[ルール (Rule) ] をクリックします。

**ステップ 4** [IP アドレス (IP address) ]または[CIDR ブロック (CIDR block) ]フィールドに、送信元または宛先 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/プレフィクス長を入力します。

**ステップ 5** [抑制の保存 (Save Suppression) ]をクリックします。

---

### 関連トピック

[Firepower システムの IP アドレス表記法](#)

## フレーム情報のフィールド

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の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再構成された 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。

### 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 パケットの場合は差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。

### Arrival Time

フレームがキャプチャされた日時。

### 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。

### 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。

### 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。

### Frame Number

差分フレーム番号。

### Frame Length

フレームの長さ (バイト単位)。

### Capture Length

キャプチャされたフレームの長さ (バイト単位)。

**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) 。

**Protocols in frame**

フレームに含まれるプロトコル。

**関連トピック**

[tag キーワード](#)

[TCP ストリームの再構成](#)

## データリンク層情報フィールド

パケットビューで、データリンク層プロトコル (たとえば、[イーサネット II (Ethernet II)] ) 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。これには、送信元ホストおよび宛先ホストの 48 ビットの Media Access Control (MAC) アドレスが含まれます。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。

**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。

**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。

### 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

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

パケットビューで、パケットに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情報を表示します。

(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。

### IPv4 ネットワーク層の情報フィールド

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

インターネットプロトコルのバージョン番号。

#### Header Length

すべての IP オプションを含む、見出しのバイト数。オプションのない IP 見出しの長さは 20 バイトです。

#### Differentiated Services Field

送信元ホストが明示的輻輳通知 (ECN) サポートする方法を示す次の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)

#### Total Length

IP 見出しを差し引いた 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的に識別する値。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。

## Flags

IP フラグメンテーションを制御する値。

[Last Fragment] 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

[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

## 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。

## 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数。

## Protocol

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。

## 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。

## 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。

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] 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化する (Blacklist Now)] または [今すぐホワイトリスト化する (Whitelist Now)] を選択します。

## IPv6 ネットワーク層の情報フィールド

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)

IPv4 で提供される差別化サービス機能と同じように、IPv6 パケット クラスまたは優先度を特定する IPv6 見出し内の Experimental 8 ビットのフィールド。未使用の場合、このフィールドはゼロに設定されます。

### Flow Label

非デフォルトの QoS またはリアルタイムサービスなどの特別なフローを特定する、1 から FFFF までの、オプションの 20 ビットの IPv6 16 進数値。未使用の場合、このフィールドはゼロに設定されます。

### 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。これは、任意の拡張子見出しを含む、IPv6 見出しに続くすべてのパケットで構成されます。

### Next Header

IPv4 プロトコルフィールドと同じ値を使用して、IPv6 見出しのすぐ後に続く、見出しの種類を特定する 8 ビットのフィールド。

### 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。

### Source

送信元ホストの 128 ビットの IPv6 アドレス。

### 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

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

**ステップ 1** 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ます。

**ステップ2** オプションで、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。

**ステップ3** [TCP パケット ビューのフィールド \(43 ページ\)](#)、[UDP パケット ビューのフィールド \(44 ページ\)](#)、または[ICMP パケット ビューフィールド \(44 ページ\)](#) の説明に従って、TCP、UDP、ICMP プロトコルのトランスポート層の内容を表示します。

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

---

## TCP パケット ビューのフィールド

ここでは、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。

### Source port

発信元のアプリケーション プロトコルを識別する番号。

### 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。

### 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。

### 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。

### 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。

### Header Length

見出しのバイト数。

### Flags

TCP セグメントの転送状態を示す 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

**UDP パケット ビューのフィールド**

- **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

**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)。

**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。

**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。

**Options**

TCP オプションの値 (存在する場合)。

**UDP パケット ビューのフィールド**

ここでは、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。

**Source port**

発信元のアプリケーション プロトコルを識別する番号。

**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。

**Length**

UDP 見出しとデータを組み合わせた長さ。

**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 フィールド**

ここでは、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。

**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

**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。

**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**

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

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化した場合は、復号化されたパケットバイトを表示できます。

## 侵入イベントのクリップボード

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。

### 関連トピック

[侵入イベント ワークフローの使用 \(24 ページ\)](#)

[侵入イベント パケット ビューの使用 \(28 ページ\)](#)

[インシデントの作成](#)

## クリップボードのレポートの生成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

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。

### 始める前に

- クリップボードに1つ以上のイベントを追加します。詳細については、[侵入イベントワークフローの使用 \(24 ページ\)](#) または [侵入イベント パケット ビューの使用 \(28 ページ\)](#) を参照してください。

**ステップ 1** [Analysis] > [Intrusions] > [Clipboard] を選択します。

**ステップ 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オンにして、[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、[すべてのレポートの生成 (Generate Report All)] をクリックします。

**ステップ 3** レポートの表示方法を指定して、[生成 (Generate)] をクリックします。

**ステップ 4** 1つ以上の出力形式を選択し、オプションで、他の設定を変更します。

**ステップ5** [生成 (Generate) ]をクリックしてから、[はい (Yes) ]をクリックします。

**ステップ6** 次の選択肢があります。

- レポート リンクをクリックして、新しいウィンドウにレポートを表示します。
- [OK]をクリックして、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。

関連トピック

[レポート テンプレート](#)

## クリップボードからのイベントの削除

スマート ライセ ンス	従来のライセンス	サポートされるデ バイス数	サポートされるド メイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

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ある場合は、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。

**ステップ1** [Analysis] > [Intrusions] > [Clipboard]を選択します。

**ステップ2** 次の選択肢があります。

- クリップボード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。
- クリップボードから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。[イベント設定 (Event Preferences) ]で[全てのアクションを確認 (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出されることに注意してください。

## 侵入イベントの統計情報の表示

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

[侵入イベントの統計情報 (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。

このページに表示される 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。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

**ステップ 1** [Overview] > [Summary] > [Intrusion Event Statistics] を選択します。

**ステップ 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。

**ステップ 3** [統計の取得 (Get Statistics)] をクリックします。

**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、[時間枠の変更](#)にある指示に従います。

## ホスト統計情報

[侵入イベント統計情報 (Intrusion Event Statistics)] ページの [ホスト統計情報 (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。Firepower Management Center 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。



**時刻 (Time)**

アプライアンスの現在の時刻。

**アップタイム (Uptime)**

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。Firepower Management Center では、[アップタイム (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。

**Disk Usage**

使用中のディスクの割合。

**Memory Usage**

使用中のシステムメモリの割合。

**Load Average**

直前の 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数。

## イベントの概要

[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、次の情報が含まれています。

**イベント**

侵入イベントデータベースのイベントの数。

**時間範囲内のイベント (Events in Time Range)**

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の割合。

**最初のイベント (First Event)**

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。

**最後のイベント (Last Event)**

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。



---

(注) Firepower Management Center で侵入イベントデータを表示中に管理対象デバイスを選択した場合は、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ません。

---

## イベント統計

[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 個のソース 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、イングレスとイーグレスのセキュリティゾーン、およびデバイス



- (注) マルチドメイン展開では、システムは、各リーフ ドメインに個別のネットワーク マップを作成します。その結果、リーフ ドメインには、ネットワーク内で一意である IP アドレスを含めることができますが、別のリーフ ドメイン内の IP アドレスと同じにすることができます。先祖ドメインでイベントの統計情報を表示すると、システムで、その IP アドレスの複数のインスタンスが繰り返し表示される場合があります。一見すると、エントリが重複しているように見えることがあります。ただし、各 IP アドレスのホストプロファイル情報までドリル ダウンすると、それらが異なるリーフ ドメインに属していることがわかります。

## 侵入イベントのパフォーマンス グラフの表示

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

[侵入イベントのパフォーマンス (Intrusion Event Performance) ] ページでは、Firepower Management Center または管理対象デバイスの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。



- (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、グラフをすばやくリロードしても、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。各グラフには、選択した時間間隔 (前月、週、日、または時間) に対応した間隔 (日、時間、または 5 分) で平均値が表示されます。平均値が 1 未満の場合は、小数値で表示されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

- ステップ 1 [Overview] > [Summary] > [Intrusion Event Performance]を選択します。
- ステップ 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。
- ステップ 3 侵入イベントのパフォーマンス統計情報グラフの種類 (51 ページ) で説明されているように、[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。
- ステップ 4 [時間範囲の選択 (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。
- ステップ 5 [グラフ (Graph)] をクリックします。
- ステップ 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。

## 侵入イベントのパフォーマンス統計情報グラフの種類

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[はい (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。

表 7: 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
Avg Bytes/Packet	n/a	各パケットに含まれる平均バイト数。	no
ECN Flags Normalized in TCP Traffic/Packet	[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
ECN Flags Normalized in TCP Traffic/Session	[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
Events/Sec	n/a	デバイスで生成された 1 秒あたりのイベント数。	no

侵入イベントのパフォーマンス統計情報グラフの種類

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
ICMPv4 Echo Normalizations	[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 Echo Normalizations	[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 Flag Normalizations	[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 (IPv4 Flags) ] ヘッダーフィールドのシングルビット [フラグメント禁止 (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 Options Normalizations	[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 Reserved Flag Normalizations	[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 (IPv4 Flags) ] ヘッダーフィールドのシングルビット [予約済み (Reserved) ] サブフィールドがクリアされた IPv4 パケットの数。	Yes
IPv4 Resize Normalizations	[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 Normalizations	[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 バイトの [差別化サービス (DS) (Differentiated Services (DS)) ] フィールド (旧 [タイプ オブ サービス (ToS) (Type of Service (TOS)) ] フィールド) がクリアされた IPv4 パケットの数。	Yes

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
IPv4 TTL Normalizations	[Normalize IPv4]、[Maximum TTL]、および [Reset TTL] を有効にします。	IPv4 存続時間 (TTL) 正規化の数。	yes
IPv6 Options Normalizations	[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 (Hop-by-Hop Options) ] または [宛先オプション (Destination Options) ] 拡張ヘッダーの [オプションタイプ (Option Type) ] 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 Normalizations	[Normalize IPv6]、[Minimum TTL]、および [Reset TTL] を有効にします。	IPv6 ホップリミット (TTL) 正規化の数。	yes
Mbits/Sec	n/a	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
Packet Resized to Fit MSS Normalizations	[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、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
Packet Resized to Fit TCP Window Normalizations	[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

侵入イベントのパフォーマンス統計情報グラフの種類

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
Percent Packets Dropped	n/a	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割合。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
RST Packets With Data Stripped Normalizations	[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
SYN Packets With Data Stripped Normalizations	[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 Header Padding Normalizations	[Normalize/Clear Option Padding Bytes] を有効にします。	オプションの埋め込みバイトが 0 に設定された TCP パケットの数。	yes
TCP No Option Normalizations	[Allow These TCP Options] を有効にして、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
TCP NS フラグの正規化 (TCP NS Flag Normalizations)	[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

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 Options Normalizations	[Allow These TCP Options] を有効にして、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
TCP Packets Blocked By Normalizations	[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 Reserved Flags Normalizations	[Normalize/Clear Reserved Bits] を有効にします。	予約ビットがクリアされたTCPパケットの数。	yes
TCP Segment Reassembly Normalizations	[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 Option Normalizations	[Allow These TCP Options] を有効にして、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 Timestamp ECR Normalizations	[Allow These TCP Options] を有効にして、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、タイムスタンプエコー応答 (TSect) 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 Urgent Pointer Normalizations	[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 (Urgent Pointer)] フィールド (2バイト) がペイロード長を超えていたため、ペイロード長に合わせて設定されたパケットの数。	Yes

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
Total Blocked Packets	[Inline Mode] または [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めて、ドロップされたパケットの総数。	no
Total Injected Packets	[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
Total TCP Filtered Packets	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
Total UDP Filtered Packets	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
Urgent Flag Cleared Normalizations	[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、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
Urgent Pointer and Urgent Flag Cleared Normalizations	[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、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
Urgent Pointer Cleared Normalizations	[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 (URG) 制御ビットが設定されていなかったため、TCPヘッダーの [緊急ポインタ (Urgent Pointer)] フィールド (16 ビット) がクリアされたパケットの数。	はい

関連トピック

[インライン正規化プリプロセッサ](#)

[インライン導入でのプリプロセッサによるトラフィックの変更](#)

[インライン展開でのドロップ動作](#)



## 侵入イベントグラフの表示

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Intrusion Admin

Firepower System 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。1 つまたはすべての管理対象デバイスについて、過去1時間から先月までの範囲の経時的な侵入イベントグラフを生成できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

**ステップ 1** [Overview] > [Summary] > [Intrusion Event Graphs] を選択します。

**ステップ 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。

**ステップ 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。

- 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

**ステップ 4** [時間範囲の選択 (Select Time Range)] で、グラフの時間範囲を選択します。

- 直近の 1 時間 (Last Hour)
- 前日 (Last Day)
- 先週 (Last Week)
- 先月 (Last Month)

**ステップ 5** [グラフ (Graph)] をクリックします。

## 侵入イベントの履歴

機能	バージョン	詳細
Syslog の接続イベントの固有識別子	6.4.0.4	syslog の [Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを一意に識別できます。これらのフィールドは、侵入イベントの syslog に含まれます。
[IntrusionPolicy] フィールドが syslog に含まれるようになりました。	6.4	侵入イベントの syslog が、イベントをトリガーした侵入ポリシーを指定するようになりました。
新しい侵入イベント検索フィールド： [CVE ID]	6.4	MITRE の Common Vulnerabilities and Exposures 識別番号で検索ができるようになりました。  変更された画面：[分析 (Analysis) ]> [侵入 (Intrusions) ]> [イベント (Events) ]> [検索の編集 (Edit Search) ]  サポート対象プラットフォーム：すべて