
# イベントの表示

ASA FirePOWER モジュールによって検査されたトラフィックについてロギングした、リアルタイム イベントを表示できます。

(注) モジュールがメモリにキャッシュするのは、直近の 100 個のイベントのみです。

詳細については、次の項を参照してください。

- ASA FirePOWER リアルタイム イベントへのアクセス（37-1 ページ）
- ASA FirePOWER イベント タイプについて（37-2 ページ）
- ASA FirePOWER イベントのイベント フィールド（37-3 ページ）
- 侵入ルールの分類（37-13 ページ）

## ASA FirePOWER リアルタイム イベントへのアクセス

いくつかの定義済みイベント ビューで ASA FirePOWER モジュールによって検出されたイベントを表示できます。または、カスタム イベント ビューを作成して、選択したイベント フィールドを表示できます。

(注) モジュールがメモリにキャッシュするのは、直近の 100 個のイベントのみです。

**ASA FirePOWER イベントを表示するには、次の手順を実行します。**

**手順 1** [モニタリング（Monitoring）] > [ASA FirePOWER モニタリング（ASA FirePOWER Monitoring）] > [リアルタイム イベント（Real-time Eventing）] の順に選択します。

**手順 2** 次の 2 つの選択肢があります。

- 表示するイベント タイプの既存のタブをクリックします。このタイプには、接続イベント、セキュリティ インテリジェンス イベント、侵入イベント、ファイル イベント、またはマルウェア イベントがあります。
- カスタム イベント ビューを作成し、ビューに含めるイベント フィールドを選択するには、[+] アイコンをクリックします。

詳細については、ASA FirePOWER イベント タイプについて（37-2 ページ）および ASA FirePOWER イベントのイベント フィールド（37-3 ページ）を参照してください。

# ASA FirePOWER イベント タイプについて

ASA FirePOWER モジュールには、5 つのイベント タイプ（接続イベント、セキュリティ インテリジェンス イベント、侵入イベント、ファイル イベント、およびマルウェア イベント）のイベント フィールドを表示する、リアルタイム イベント ビューがあります。

### 接続イベント

*接続イベント*と呼ばれる接続ログには、検出されたセッションに関するデータが含まれています。個々の接続イベントで入手可能な情報はいくつかの要因に応じて異なりますが、一般的には次のものがあります。

- タイムスタンプ、送信元と宛先の IP アドレス、入出力ゾーン、接続を処理したデバイスなど、基本的な接続特性
- アプリケーション、要求される URL、または接続に関連付けられているユーザなど、システムによって検出または推測される追加の接続特性
- どのポリシーのどのアクセス コントロール ルール（または他の設定）がトラフィックを処理したか、接続が許可またはブロックされているかなど、接続がログに記録された理由に関するメタデータ

アクセス コントロールでさまざまな設定を行うことで、ログに記録する接続の種類、接続をログに記録する時期、およびデータを保存する場所をきめ細かく制御できます。アクセス コントロール ポリシーが正常に処理できる接続をログに記録できます。接続のロギングは、次の状況で有効にすることができます。

- 接続がレピュテーション ベースのセキュリティ インテリジェンス機能によってブラックリスト登録（ブロック）またはモニタされた場合
- 接続がアクセス コントロール ルールまたはアクセス コントロールのデフォルト アクションによって処理された場合

設定するロギングに加えて、禁止されたファイル、マルウェア、または侵入の試みをシステムが検出した場合には、ほとんどの接続を自動的にログに記録します。

### セキュリティ インテリジェンス イベント

セキュリティ インテリジェンス ロギングを有効にすると、ブラックリストの一致によって*セキュリティ インテリジェンス イベント*および接続イベントが自動的に生成されます。セキュリティ インテリジェンス イベントは特殊なタイプの接続イベントで、単独で表示して分析できます。セキュリティ インテリジェンス ブラックリスト登録の決定を含む、接続ロギングの設定の詳細については、ネットワーク トラフィックの接続のロギング（36-1 ページ）を参照してください。

ヒント　特に断りがない限り、接続イベントに関する一般情報も、セキュリティ インテリジェンス イベントに関係します。セキュリティ インテリジェンスの詳細については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録（5-1 ページ）を参照してください。

### 侵入イベント

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、侵入の可能性を特定すると*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、時刻、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。

### ファイル イベント

*ファイル イベント*は、システムがネットワーク トラフィック内で検出した（およびオプションでブロックした）ファイルを表します。

システムは、現在適用されているファイル ポリシーのルールに従って、管理対象デバイスがネットワーク トラフィック内のファイルを検出またはブロックしたときに生成されたファイル イベントを記録します。

### マルウェア イベント

*マルウェア イベント*は、システムがネットワーク トラフィック内で検出した（およびオプションでブロックした）マルウェア ファイルを表します。

Malware ライセンスを使用すると、ASA FirePOWER モジュールは全体的なアクセス コントロール設定の一部として、ネットワーク トラフィック内のマルウェアを検出できます。ファイル ポリシーの概要と作成（35-4 ページ）を参照してください。

以下のシナリオでは、マルウェア イベントが生成される可能性があります。

- 管理対象デバイスが一連の特定のファイル タイプのいずれかを検出すると、ASA FirePOWER モジュールはマルウェア クラウド ルックアップを実行します。これにより、ファイル性質として `Malware`、`Clean`、または `Unknown` が ASA FirePOWER モジュールに返されます。
- ASA FirePOWER モジュールがクラウドとの接続を確立できない場合や、その他の理由でクラウドが使用できない場合、ファイル性質は `Unavailable` になります。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。
- クリーン リストに含まれているファイルを管理対象デバイスが検出した場合、ASA FirePOWER モジュールはファイル性質として `Clean` をそのファイルに割り当てます。

ASA FirePOWER モジュールは、ファイルの検出と性質のレコードを、他のコンテキスト データとともにマルウェア イベントとして記録します。

ネットワーク トラフィックで検出され、ASA FirePOWER モジュールによってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。これは、システムがファイル内のマルウェアを検出するために、まずそのファイル自体を検出する必要があるためです。

# ASA FirePOWER イベントのイベント フィールド

### アクション（Action）

接続イベントまたはセキュリティ インテリジェンス イベントの場合、接続をロギングしたアクセス コントロール ルールまたはデフォルト アクションに関連付けられたアクション。

- [許可（Allow）] は、明示的に許可されてユーザがバイパスする、インタラクティブにブロックされる接続を表します。
- [信頼（Trust）] は、信頼できる接続を表します。最初のパケットが信頼ルールによって検出された TCP 接続のみ、接続終了イベントを生成します。システムは、最後のセッション パケットの 1 時間後にイベントを生成します。
- [ブロック（Block）] と [リセットしてブロック（Block with reset）] は、ブロックされた接続を表します。さらにシステムは、[ブロック（Block）] アクションを、セキュリティ インテリジェンスによってブラックリストに記載された接続、侵入ポリシーによってエクスプロイトが検出された接続、ファイル ポリシーによってファイルがブロックされた接続と関連付けます。

- [インタラクティブ ブロック（Interactive Block）] と [リセットしてインタラクティブ ブロック（Interactive Block with reset）] は、システムがインタラクティブ ブロック ルールを使用して最初にユーザの HTTP 要求をブロックしたときにロギングできる接続開始イベントをマークします。システムが表示する警告ページでユーザがクリック操作をすると、そのセッションについてロギングするその他の接続イベントは、アクションが [許可（Allow）] になります。
- [デフォルト アクション（Default Action）] は、デフォルト アクションによって接続が処理されたことを示します。
- セキュリティ インテリジェンスによってモニタされている接続の場合、そのアクションは、接続によってトリガーされる最初の（モニタ以外の）アクセス コントロール ルールのアクションであるか、またはデフォルト アクションです。同様に、モニタ ルールに一致するトラフィックは常に後続のルールまたはデフォルト アクションによって処理されるため、モニタ ルールによってロギングされた接続と関連付けられたアクションが [モニタ（Monitor）] になることはありません。

ファイル イベントまたはマルウェア イベントの場合、ファイルが一致したルールのルール アクションに関連付けられているファイル ルール アクションと、関連するファイル ルール アクションのオプション。

**許可された接続（Allowed Connection）**

システムがイベントのトラフィック フローを許可したかどうか。

**アプリケーション（Application）**

接続で検出されたアプリケーション。

**アプリケーションのビジネスとの関連性（Application Business Relevance）**

接続で検出されたアプリケーション トラフィックに関連するビジネス関連性：`Very High`、`High`、`Medium`、`Low`、または `Very Low`。接続で検出されたアプリケーションのタイプごとに、関連するビジネス関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

**アプリケーション カテゴリ（Application Categories）**

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カテゴリ。

**アプリケーションのリスク（Application Risk）**

接続で検出されたアプリケーション トラフィックに関連するリスク：`Very High`、`High`、`Medium`、`Low`、または `Very Low`。接続で検出された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。このフィールドでは、それらのうち最も高いものが表示されます。

**アプリケーション タグ（Application 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タグ。

**ブロック タイプ（Block Type）**

イベントのトラフィック フローと一致するアクセス コントロール ルールで指定されたブロックのタイプ。ブロックまたはインタラクティブ ブロック。

**クライアント（Client）**

接続で検出されたクライアント アプリケーション。

接続に使用されている特定のクライアントをシステムが特定できなかった場合、このフィールドは汎用的な名称としてアプリケーション プロトコル名の後に client を付加して FTP client などと表示します。

**クライアントのビジネスとの関連性（Client Business Relevance）**

接続で検出されたクライアント トラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたクライアントのタイプごとに、ビジネスとの関連性が関連付けられています。このフィールドは、最も低いもの（関連性が最も低い）を表示します。

**クライアント カテゴリ（Client Categories）**

クライアントの機能を理解するのに役立つ、トラフィックで検出されたクライアントの特性を示すカテゴリ。

**クライアント リスク（Client Risk）**

接続で検出されたクライアント トラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出されたクライアントのタイプごとに、リスクが関連付けられています。このフィールドは、最も高いものを表示します。

**クライアント タグ（Client Tag）**

クライアントの機能を理解するのに役立つ、トラフィックで検出されたクライアントの特性を示すタグ。

**クライアント バージョン（Client Version）**

接続で検出されたクライアントのバージョン。

**接続（Connection）**

内部的に生成されたトラフィック フローの固有 ID。

**接続ブロックタイプ インジケータ（Connection Blocktype Indicator）**

イベントのトラフィック フローと一致するアクセス コントロール ルールで指定されたブロックのタイプ。ブロックまたはインタラクティブ ブロック。

**接続バイト（Connection Bytes）**

接続の合計バイト数。

**接続時間（Connection Time）**

接続の開始時刻。

**接続タイムスタンプ（Connection Timestamp）**

接続が検出された時刻。

**コンテキスト（Context）**

トラフィックが通過したセキュリティ コンテキスト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 デバイスだけです。

**拒否された接続（Denied Connection）**

システムがイベントのトラフィック フローを拒否したかどうか。

**宛先の国または大陸（Destination Country and Continent）**

受信ホストの国および大陸。

**宛先 IP（Destination IP）**

受信ホストが使用する IP アドレス。

**宛先ポート、宛先ポート コード、宛先ポート/ICMP コード（Destination Port, Destination Port Icode, Destination Port/ICMP Code）**

セッション レスポンダが使用する宛先ポートまたは ICMP コード。

**方向（Direction）**

ファイルの送信方向。

**傾向（Disposition）**

以下のファイル性質のいずれかです。

- マルウェア（Malware）：クラウドでそのファイルがマルウェアとして分類されていることを示します。
- クリーン（Clean）：クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。
- 不明（Unknown）：クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。ファイルは分類されていません。
- カスタム検出（Custom Detection）：ユーザがカスタム検出リストにファイルを追加したことを示します。
- 使用不可（Unavailable）：ASA FirePOWER モジュールがマルウェア クラウド ルックアップを実行できなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。
- N/A：[ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] ルールがファイルを処理し、ASA FirePOWER モジュールがマルウェア クラウド ルックアップを行わなかったことを示します。

**出力インターフェイス（Egress Interface）**

接続に関連付けられた出力インターフェイス。展開環境に非同期のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインターフェイス セットに属する場合があることに注意してください。

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

接続に関連付けられた出力セキュリティ ゾーン。

**イベント（Event）**

イベントのタイプ。

**イベント（マイクロ秒）（Event Microseconds）**

イベントが検出された時刻（マイクロ秒単位）。

**イベント（秒）（Event Seconds）**

イベントが検出された時刻（秒単位）。

**イベント タイプ（Event Type）**
イベントのタイプ。

**ファイル カテゴリ（File Category）**
ファイル タイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイル など）。

**ファイル イベント タイムスタンプ（File Event Timestamp）**
ファイルまたはマルウェア ファイルが作成された日時。

**ファイル名（File Name）**
ファイルまたはマルウェア ファイルの名前。

**ファイル SHA256（File SHA256）**
ファイルの SHA-256 ハッシュ値。

**ファイル サイズ（File size）**
ファイルまたはマルウェア ファイルのサイズ（KB 単位）。

**ファイル タイプ（File Type）**
ファイルまたはマルウェア ファイルのファイル タイプ（HTML や MSEXE など）。

**ファイル/マルウェア ポリシー（File/Malware Policy）**
イベントの生成に関連付けられているファイル ポリシー。

**ファイルログ ブロックタイプ インジケータ（Filelog Blocktype Indicator）**
イベントのトラフィック フローと一致するファイル ルールで指定されたブロックのタイプ。ブロックまたはインタラクティブ ブロック。

**ファイアウォール ポリシー ルール/SI カテゴリ（Firewall Policy Rules/SI Category）**
接続でブラックリストに記載された IP アドレスを表すか、もしくはそれを含む、ブラックリストに記載されたオブジェクトの名前。セキュリティ インテリジェンスのカテゴリは、ネットワーク オブジェクトまたはグループ、グローバル ブラックリスト、カスタム セキュリティ インテリジェンスのリストまたはフィード、またはインテリジェンス フィードのカテゴリのいずれかの名前にすることができます。[理由（Reason）] が [IP ブロック（IP Block）] または [IP モニタ（IP Monitor）] の場合にのみ、このフィールドに値が入力されることに注意してください。セキュリティ インテリジェンス イベントのビューでは、エントリに必ず理由が表示されます。

**ファイアウォール ルール（Firewall Rule）**
接続を処理したアクセス コントロール ルールまたはデフォルト アクションと、その接続に一致した最大 8 つのモニタ ルール。

**最初のパケット（First Packet）**
セッションの最初のパケットが検出された日時。

**HTTP リファラ（HTTP Referrer）**

接続で検出された HTTP トラフィックの要求 URL のリファラを示す HTTP リファラ（他の URL へのリンクを提供した Web サイト、他の URL からリンクをインポートした Web サイトなど）。

**IDS の分類（IDS 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。

**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。

**影響フラグ（Impact Flag）**

「影響（Impact）」を参照してください。

**入力インターフェイス（Ingress Interface）**

接続に関連付けられた入力インターフェイス。展開環境に非同期のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインターフェイス セットに属する場合があることに注意してください。

**入力セキュリティ ゾーン（Ingress Security Zone）**

接続に関連付けられた入力セキュリティ ゾーン。

**イニシエータ バイト数（Initiator Bytes）**

セッション イニシエータが送信した合計バイト数。

**イニシエータの国または大陸（Initiator Country and Continent）**

ルーティング可能な IP が検出された場合の、セッションを開始したホスト IP アドレスに関連付けられた国および大陸。

**イニシエータ IP（Initiator IP）**

セッション レスポンダを開始したホスト IP アドレス（および DNS 解決が有効化されている場合はホスト名）。

**イニシエータ パケット（Initiator Packets）**

セッション イニシエータが送信した合計パケット数。

**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。

**IPS ブロックタイプ インジケータ（IPS Blocktype Indicator）**

イベントのトラフィック フローと一致する侵入ルールのアクション。

**最後のパケット（Last Packet）**

セッションの最後のパケットが検出された日時。

**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。

**マルウェア ブロックタイプ インジケータ（Malware Blocktype Indicator）**

イベントのトラフィック フローと一致するファイル ルールで指定されたブロックのタイプ。ブロックまたはインタラクティブ ブロック。

**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。

マルウェア イベントの場合は、マルウェア イベントに関連付けられている追加情報。ネットワークベースのマルウェア イベントの場合、このフィールドにデータが入れられるのは、性質が変更されたファイルだけです。

**モニタ ルール（Monitor Rules）**

その接続で一致する 8 つまでのモニタ ルール。

**Netbios ドメイン（Netbios Domain）**

セッションで使用された NetBIOS ドメイン。

**元のクライアントの国と大陸（Original Client Country and Continent）**

元のクライアントの IP アドレスが属する国。この値を取得するために、システムは元のクライアント IP アドレスを X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーから抽出し、それを位置情報データベース（GeoDB）を使用して国にマップします。このフィールドに入力するには、元のクライアントに基づいてプロキシ トラフィックを処理するアクセス コントロール ルールを有効にする必要があります。

**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 ヘッダーからの、元のクライアント IP アドレス。このフィールドに入力するには、元のクライアントに基づいてプロキシ トラフィックを処理するアクセス コントロール ルールを有効にする必要があります。

**ポリシー(Policy)**

イベントの生成に関連付けられているアクセス コントロール ポリシー、侵入ポリシー、またはネットワーク分析ポリシー(NAP)(ある場合)。

**ポリシー リビジョン(Policy Revision)**

イベントの生成に関連付けられているアクセス コントロール ポリシー、ファイル ポリシー、侵入ポリシー、またはネットワーク分析ポリシー(NAP)(ある場合)のリビジョン。

**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。

**プロトコル(Protocol)**

接続で検出されたプロトコル。

**プロトコル(Protocol)**

次の場合に接続がロギングされた 1 つまたは複数の原因。

- [ユーザ バイパス(User Bypass)] は、システムが最初はユーザの HTTP 要求をブロックしたが、ユーザが警告ページでクリック操作をして、最初に要求していたサイトへ進むのを選択したことを示します。[ユーザ バイパス(User Bypass)] の原因は必ず [許可(Allow)] のアクションと対として組み合わされます。
- [IP ブロック(IP Block)] は、システムがセキュリティ インテリジェンス データに基づいて、インスペクションなしで接続を拒否したことを示します。[IP ブロック(IP Block)] の原因は必ず [ブロック(Block)] のアクションと対として組み合わされます。
- [IP モニタ(IP Monitor)] は、システムがセキュリティ インテリジェンス データに基づいて接続を拒否するはずでしたが、ユーザが接続を拒否せずモニタするように設定したことを示します。
- [ファイル モニタ(File Monitor)] は、システムが接続において特定のファイルの種類を検出したことを示します。
- [ファイル ブロック(File Block)] は、ファイルまたはマルウェア ファイルが接続に含まれており、システムがその送信を防いだことを示します。[ファイル ブロック(File Block)] の理由は必ず [ブロック(Block)] のアクションと対として組み合わされます。
- [ファイル カスタム検出(File Custom Detection)] は、カスタム検出リストにあるファイルが接続に含まれており、システムがその送信を防いだことを示します。
- [ファイル復帰許可(File Resume Allow)] は、ファイル送信がはじめに [ファイル ブロック(Block Files)] または [マルウェア ブロック(Block Malware)] ファイル ルールによってブロックされたことを示します。ファイルを許可する新しいアクセス コントロール ポリシーが適用された後、HTTP セッションが自動的に再開しました。この原因は、インライン構成のみで表示されることに注意してください。
- [ファイル復帰ブロック(File Resume Block)] は、ファイル送信がはじめに [ファイル検出(Detect Files)] または [マルウェア クラウド ルックアップ(Malware Cloud Lookup)] ファイル ルールによって許可されたことを示します。ファイルをブロックする新しいアクセス コントロール ポリシーが適用された後、HTTP セッションが自動的に停止しました。この原因は、インライン構成のみで表示されることに注意してください。
- [侵入ブロック(Intrusion Block)] は、接続で検出されたエクスプロイト(侵入ポリシー違反)をシステムがブロックしたか、ブロックするはずだったことを示します。[侵入ブロック(Intrusion Block)] の原因は、ブロックされたエクスプロイトの場合は [ブロック(Block)]、ブロックされるはずだったエクスプロイトの場合は [許可(Allow)] のアクションと対として組み合わされます。

- [侵入モニタ（Intrusion Monitor）] は、接続で検出されたエクスプロイトをシステムが検出したものの、ブロックしなかったことを示します。これは、トリガーされた侵入ルールの状態が [イベントを生成する（Generate Events）] に設定されている場合に発生します。
- [コンテンツ制限（Content Restriction）] は、セーフサーチまたは YouTube EDU 機能のいずれかに関連したコンテンツ制限を実施するために、システムがパケットを変更したことを示します。

**受信時間（Receive Times）**

宛先ホストまたはレスポンダがイベントに応答した時刻。

**参照ホスト（Referenced Host）**

接続のプロトコルが DNS、HTTP、または HTTPS の場合、このフィールドにはそれぞれのプロトコルが使用していたホスト名が表示されます。

**レスポンダ バイト数（Responder Bytes）**

セッション レスポンダが送信した合計バイト数。

**レスポンダの国または大陸（Responder Country and Continent）**

ルーティング可能な IP が検出された場合の、セッション レスポンダのホスト IP アドレスに関連付けられた国および大陸。

**レスポンダ パケット（Responder Packets）**

セッション レスポンダが送信した合計パケット数。

**レスポンダ IP（Responder IP）**

セッション イニシエータに応答したホスト IP アドレス（および DNS 解決が有効化されている場合はホスト名）。

**セキュリティ グループ タグの名前（Security Group Tag Name）**

接続に関係するパケットのセキュリティ グループ タグ（SGT）属性。SGT は、信頼ネットワーク内での、トラフィックの送信元の権限を指定します。セキュリティ グループ アクセス（Cisco TrustSec と Cisco ISE の両方に共通の機能）は、パケットがネットワークに入るときに属性を適用します。

**シグネチャ（Signature）**

イベントのトラフィックと一致する侵入ルールのシグネチャ ID。

**ソースの国または大陸（Source Country and Continent）**

送信元ホストの国および大陸。

**ソース IP（Source IP）**

侵入イベントで送信元ホストが使用する IP アドレス。

**送信元または宛先（Source or Destination）**

イベントの接続を送信元/宛先とするホスト。

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

セッション イニシエータが使用する送信元ポートまたは ICMP タイプ。

**TCP フラグ（TCP Flags）**

接続で検出された TCP フラグ。

**URL**

セッション中にモニタ対象のホストによって要求された URL。

**URL カテゴリ（URL Category）**

セッション中にモニタ対象のホストによって要求された URL に関連付けられているカテゴリ（使用可能な場合）。

**URL レピュテーション（URL Reputation）**

セッション中にモニタ対象のホストによって要求された URL に関連付けられているレピュテーション（使用可能な場合）。

**URL レピュテーション スコア（URL Reputation Score）**

セッション中にモニタ対象のホストによって要求された URL に関連付けられているレピュテーション スコア（使用可能な場合）。

**ユーザ（User）**

イベントが発生したホスト（**受信 IP**）のユーザ

**ユーザ エージェント（User Agent）**

接続で検出された HTTP トラフィックから取得したユーザ エージェント アプリケーションの情報。

**VLAN**

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。

**Web アプリケーションのビジネスとの関連性（Web App Business Relevance）**

接続で検出された Web アプリケーション トラフィックに関連するビジネス関連性：`Very High`、`High`、`Medium`、`Low`、または `Very Low`。接続で検出された Web アプリケーションのタイプごとに、ビジネスとの関連性が関連付けられています。このフィールドは、最も低いもの（関連性が最も低い）を表示します。

**Web アプリケーションのカテゴリ（Web App Categories）**

Web アプリケーションの機能を理解するのに役立つ、トラフィックで検出された Web アプリケーションの特性を示すカテゴリ。

**Web アプリケーションのリスク（Web App Risk）**

接続で検出された Web アプリケーション トラフィックに関連するリスク：`Very High`、`High`、`Medium`、`Low`、または `Very Low`。接続で検出された Web アプリケーションのタイプごとに、リスクが関連付けられています。このフィールドは、最も高いものを表示します。

**Web アプリケーションのタグ（Web App Tag）**

Web アプリケーションの機能を理解するのに役立つ、トラフィックで検出された Web アプリケーションの特性を示すタグ。

**Web アプリケーション（Web Application）**

トラフィックで検出された Web アプリケーション。

# 侵入ルールの分類

侵入ルールには、攻撃の分類が含まれています。次の表に、それぞれの分類の名前と番号を示します。

*表 37-1　ルールの分類*

| 番号 | 分類名 | 説明 |
|---|---|---|
| 1 | not-suspicious | 不審ではないトラフィック |
| 2 | unknown | 不明なトラフィック |
| 3 | bad-unknown | 有害な可能性のあるトラフィック |
| 4 | attempted-recon | 情報漏えいが試行された |
| 5 | successful-recon-limited | 情報漏えいが発生 |
| 6 | successful-recon-largescale | 大規模な情報漏えい |
| 7 | attempted-dos | サービス妨害が試行された |
| 8 | successful-dos | サービス妨害（DoS） |
| 9 | attempted-user | ユーザ特権の獲得が試行された |
| 10 | unsuccessful-user | ユーザ特権の獲得が失敗した |
| 11 | successful-user | ユーザ特権の獲得に成功 |
| 12 | attempted-admin | 管理者特権の獲得が試行された |
| 13 | successful-admin | 管理者特権の獲得に成功 |
| 14 | rpc-portmap-decode | RPC クエリのデコード |
| 15 | shellcode-detect | 実行可能コードが検出された |
| 16 | string-detect | 疑わしい文字列が検出された |
| 17 | suspicious-filename-detect | 疑わしいファイル名が検出された |
| 18 | suspicious-login | 疑わしいユーザ名を使用したログイン試行が検出された |
| 19 | system-call-detect | システム コールが検出された |
| 20 | tcp-connection | TCP 接続が検出された |
| 21 | trojan-activity | ネットワーク トロイの木馬が検出された |
| 22 | unusual-client-port-connection | 通常とは異なるポートをクライアントが使用していた |
| 23 | network-scan | ネットワーク スキャンの検出 |
| 24 | denial-of-service | サービス妨害攻撃の検出 |
| 25 | non-standard-protocol | 非標準プロトコルまたはイベントの検出 |
| 26 | protocol-command-decode | 一般的なプロトコル コマンド デコード |
| 27 | web-application-activity | 脆弱な可能性のある Web アプリケーションへのアクセス |
| 28 | web-application-attack | Web アプリケーション攻撃 |
| 29 | misc-activity | その他のアクティビティ |
| 30 | misc-attack | その他の攻撃 |

*表 37-1　ルールの分類(続き)*

| 番号 | 分類名 | 説明 |
|---|---|---|
| 31 | icmp-event | 一般的な ICMP イベント |
| 32 | inappropriate-content | 不適切な内容が検出された |
| 33 | policy-violation | 企業プライバシー侵害の可能性 |
| 34 | default-login-attempt | デフォルトのユーザ名とパスワードによるログイン試行 |
| 35 | sdf | 機密データ |
| 36 | malware-cnc | 既知のマルウェア コマンドと制御トラフィック |
| 37 | client-side-exploit | 既知のクライアント側エクスプロイト試行 |
| 38 | file-format | 既知の悪意のあるファイルまたはファイル ベースのエクスプロイト |