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対してロギングされたリアルタイム 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。

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 フィールドを表示することができます。

（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。

ステップ 1 [Monitoring] > [ASA FirePOWER Monitoring] > [Real-time Eventing] の順に選択します。

ステップ 2 次の 2 つの選択肢があります。

- 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 イベントから表示するイベントのタイプの既存のタブをクリックします。
- 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 （2 ページ）およびASA FirePOWER イベントのイベント フィールド （4 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 モジュールでは、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）からのイベント フィールドを表示するリアルタイム イベント ビューが提供されます。

Connection Events

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よって決まりますが、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
- ポリシーがトラフィックを処理したアクセス コントロール ルール（または他の設定）、接続が許可またはブロックされているかどうかなど、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、ログする接続の種類、接続をログする時期、およびデータを保存する場所のきめ細かい制御を行うことができます。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ロックまたはモニタされる場合
- 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、システムは禁止されたファイル、マルウェア、または侵入の試みを検出した場合に、ほとんどの接続を自動的にログに記録します。

Security Intelligence Events

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、ブロ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、個別に表示および分析できます。セキュリティインテリジェンスによるブロックの決定を含む、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を参照してください。

ヒント　特に明記されていない限り、接続イベントに関する一般情報もまたセキュリティ インテリジェンス イベントに関連します。セキュリティ インテリジェンスの詳細については、レピュテーションベースのルールによるトラフィックの制御 を参照してください。

Intrusion Events

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悪意のあるアクティビティについて、ネットワークを通過するパケットを検査します。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。

File Events

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（さらに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。

Malware Events

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（さらに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。

マルウェア 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 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。この性質で見られる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 モジュールは他のコンテキスト データとともに、ファイルの検出と性質のレコードをマルウェア 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、ファイル内のマルウェアを検出するために、システムは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

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。
- [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。
- [Block] と [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ロックされた接続、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、および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にも関連付けます。
- [Interactive Block] と [Interactive Block with reset] は、システムが Interactive Block 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示します。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 [Allow] になります。
- [Default Action] は、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。
- セキュリティインテリジェンスによって監視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監視以外のアクセス コントロール ルールのアクションか、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に関連付けられたアクションが [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。

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。

Application

接続で検出されたアプリケーション。

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付けられたビジネスとの関連性：[Very High]、[High]、[Medium]、[Low]、[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。

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。

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付けられたリスク：[Very High]、[High]、[Medium]、[Low]、[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。

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。

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。[Block] または [Interactive Block]。

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い場合、このフィールドに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 を付加した形で、FTP client などと表示されます。

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付けられたビジネスとの関連性：[Very High]、[High]、[Medium]、[Low]、[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。

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。

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付けられたリスク：[Very High]、[High]、[Medium]、[Low]、[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。

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。

Client Version

接続で検出されたクライアントのバージョン。

Connection

内部的に生成されたトラフィック フローの固有 ID。

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。[Block] または [Interactive Block]。

Connection Bytes

接続の合計バイト数。

Connection Time

接続の開始時刻。

Connection Timestamp

接続が検出された時刻。

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。マルチ コンテキスト モードのデバイスでは、システムはこのフィールドにのみ入力することに注意してください。

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。

Destination Country and Continent

受信ホストの国および大陸。

Destination IP

受信ホストが使用する IP アドレス。

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。

Direction

ファイルの送信方向。

Disposition

以下のファイル性質のいずれかです。

- Malware：クラウドがマルウェアとしてファイルを分類したことを示します。
- Clean は、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。
- Unknown は、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。
- [Custom Detection] は、ファイルをユーザがカスタム検出リストに追加したことを示します。
- 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。この性質で見られる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：ファイル検出またはファイル ブロック 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。

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。

Egress Security Zone

接続に関連付けられた出力セキュリティ ゾーン。

Event

イベントのタイプ。

Event Microseconds

イベントが検出された時刻（マイクロ秒単位）。

Event Seconds

イベントが検出された時刻（秒単位）。

Event Type

イベントのタイプ。

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）。

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。

File Name

ファイルまたはマルウェア ファイルの名前。

File SHA256

ファイルの SHA-256 ハッシュ値。

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）。

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）。

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。

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。[Block] または [Interactive Block]。

Firewall Policy Rules/SI Category

接続でブロックされた IP アドレスを表すか、またはそれを含む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、グローバルブロックリスト、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、あるい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できます。[Reason] が [IP Block] または [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、エントリに必ず原因が表示されます。

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 Monitor ルール。

First Packet

セッションの最初のパケットが検出された日時。

HTTP Referrer

接続で検出された HTTP トラフィックの要求 URL の参照元を示す HTTP 参照元（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 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、表 1 : ルールの分類 （15 ページ）の表を参照してください。

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。

Impact Flag

「Impact」を参照してください。

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。

Ingress Security Zone

接続に関連付けられた入力セキュリティ ゾーン。

Initiator Bytes

セッション イニシエータが送信した合計バイト数。

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。

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）。

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。

Inline Result

次のいずれかが必要です。

- 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。[Drop when Inline] 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 [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 [Drop and Generate Events] に設定されて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 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。

Last Packet

セッションの最後のパケットが検出された日時。

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。

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。[Block] または [Interactive Block]。

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。

Monitor Rules

その接続で一致する 8 つまでのモニタ ルール。

Netbios Domain

セッションで使用された NetBIOS ドメイン。

Num Ioc

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。

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、それを地理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。

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。

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）。

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、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。

Priority

Cisco VRT で指定されたイベントの優先順位。

Protocol

接続で検出されたプロトコル。

Reason

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。

- [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ことを選択したことを示します。[User Bypass] の原因は必ず [Allow] のアクションとペアになります。

- [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 Block] の原因は必ず [Block] のアクションとペアになります。
- [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監視するように設定したことを示します。
- [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。
- [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。[File Block] の原因は必ず [Block] のアクションとペアになります。
- [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。
- [File Resume Allow] は、ファイル送信がはじめにファイル ブロックまたはマルウェア ブロック 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。その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で、HTTP セッションは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。
- [File Resume Block] は、ファイル送信がはじめにファイル検出または マルウェア クラウド ルックアップ ファイル ルールによって許可されたことを示します。その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で、HTTP セッションは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。
- [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）] の理由は、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。
- [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 [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。

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。

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。

Responder Bytes

セッション レスポンダが送信した合計バイト数。

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。

Responder Packets

セッション レスポンダが送信した合計パケット数。

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）。

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。

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。

Source Country and Continent

送信元ホストの国および大陸。

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。

Source or Destination

イベントの接続を送信元/宛先とするホスト。

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 Flags

接続で検出された TCP フラグ。

URL

セッション中に監視対象のホストによって要求された URL。

URL Category

セッション中に監視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 Reputation

セッション中に監視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 Reputation Score

セッション中に監視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）。

User

イベントが発生したホスト（**受信 IP**）のユーザ

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 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付けられているビジネスとの関連性：[Very High]、[High]、[Medium]、[Low]、[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 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 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付けられたリスク：[Very High]、[High]、[Medium]、[Low]、[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 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 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 *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	サービス拒否が試行された
8	successful-dos	サービス拒否が発生
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

番号	分類名	説明
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	サービス拒否攻撃の検出
25	non-standard-protocol	標準的でない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
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 exploit 試行
38	file-format	既知の有害ファイルまたはファイル ベースの exploit