デバイスのモニタリング

システムには、デバイスおよびデバイスを通過するトラフィックをモニタするために使用できるダッシュボードとイベント ビューアが含まれています。

トラフィック統計情報を取得するためのロギングの有効化

モニタリング ダッシュボードおよびイベント ビューアを使用して、幅広い種類のトラフィック統計をモニタできます。これには、ロギングを有効にして、収集する統計の種類をシステムに指示する必要があります。

次のロギング タイプを個々のアクセス ルールに対して有効化することで、オプションの統計情報が収集され、イベントが生成されます。

- 接続ロギング：接続の終了時にロギングが行われるため、接続に関するほとんどの情報を取得できます。接続の開始時にロギングを行うこともできますが、これらのイベントで得られる情報は不完全です。接続ロギングはデフォルトで無効になっているため、追跡したいトラフィックを対象とする個々のルール（およびデフォルト アクション）に対し、接続ロギングを有効化する必要があります。
- ファイル ロギング：検出されたファイルについての情報を収集するには、ファイル ロギングを有効化する必要があります。アクセス ルールでファイル ポリシーを選択すると、ファイル ロギングは自動的に有効化されますが、無効にすることもできます。

設定したロギングに加え、禁止されたファイルやマルウェアが検出された場合、または侵入が試みられた場合には、ほとんどの接続が自動的に記録されます（接続終了時）。ただし、デフォル

トアクションによって対処される侵入イベントは例外です。これらの侵入イベントを確認するには、デフォルト アクションに対して接続ロギングを有効化する必要があります。

ヒント

ロギングの設定、および関連する統計情報の評価について検討する場合は、以下のヒントを参考にしてください。

- アクセス コントロール ルールでトラフィックを許可すると、関連付けられた侵入ポリシーまたはファイル ポリシー（またはその両方）を使用して、さらにトラフィックをのインスペクションを実行し、トラフィックが最終宛先に到達する前に、侵入、禁止されたファイル、およびマルウェアをブロックすることができます。ただし、デフォルトでは、ファイルおよび侵入のインスペクションは暗号化されたペイロードでは無効になっていることに注意してください。侵入ポリシーまたはファイル ポリシーに基づき、接続をブロックする根拠が得られた場合は、接続ログの設定にかかわらず、接続終了イベントがただちに記録されます。ロギングの許可された接続からは、ネットワーク内のトラフィックに関するほとんどの統計情報を収集できます。
- 信頼されている接続は、信頼アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルトアクションによって処理される接続です。しかし、信頼されている接続に対しては、ディスカバリ データ、侵入、禁止されたファイルやマルウェアのインスペクションは行われません。したがって、信頼されている接続の接続イベントには、限られた情報が含まれます。
- トラフィックをブロックしたアクセス コントロール ルールおよびアクセス コントロールポリシーのデフォルトアクションに対しては、接続開始イベントが自動的に記録されます。一致するトラフィックは、追加のインスペクションなしで拒否されます。
- サービス妨害（DoS）攻撃時にブロックされたTCP接続のロギングは、システムパフォーマンスに影響し、複数の類似のイベントでデータベースが圧倒される場合があります。ブロック ルールに対してロギングを有効化する場合は、ルールによってインターネット側のインターフェイスを通過するトラフィックを監視するのか、またはDoS攻撃に対して脆弱な他のインターフェイスを監視するのかを事前に検討します。

トラフィックおよびシステムダッシュボードのモニタリング

システムには、デバイスを通過するトラフィックとセキュリティ ポリシーの結果を分析するために使用できるいくつかのダッシュボードが含まれています。この情報を使用して、設定の全体的な有効性を評価するとともに、ネットワークに関する問題を特定して解決します。

（注） トラフィック関連のダッシュボードで使用されるデータは、接続またはファイル ロギングを可能にするアクセス コントロール ルールから収集されます。ダッシュボードには、ロギングが有効になっていないルールに一致するトラフィックは反映されません。必ず、重要な情報がログに記録されるようにルールを設定してください。また、ユーザ情報は、ユーザ アイデンティティを収集するためのアイデンティティ ルールを設定する場合にのみ使用できます。最後に、侵入、ファイル、マルウェア、および Web カテゴリ情報は、それらの機能のライセンスがあり、それらの機能を使用するルールを設定する場合にのみ使用できます。

手順

ステップ 1 メイン メニューの [モニタリング（Monitoring）] をクリックして [ダッシュボード（Dashboards）] ページを開きます。
定義済みの時間範囲（過去 1 時間、過去 1 週間など）を選択するか、特定の開始時間と終了時間によるカスタム時間範囲を定義して、ダッシュボードのグラフとテーブルに表示されるデータを制御できます。

トラフィック関連のダッシュボードには、次のタイプの表示があります。

- 上位 5 つの棒グラフ：これらは、[ネットワークの概要（Network Overview）] ダッシュボードに表示され、ダッシュボードテーブルの項目をクリックすると表示される項目ごとの概要ダッシュボードにも表示されます。[トランザクション（Transactions）] の数と [データ使用量（Data Usage）]（送受信された総バイト数）の間で情報を切り替えることができます。すべてのトランザクション、許可トランザクション、拒否トランザクションの表示を切り替えることもできます。[詳細表示（View More）] リンクをクリックすると、グラフに関連付けられたテーブルが表示されます。
- テーブル：テーブルには、特定タイプの項目（アプリケーション、Web カテゴリなど）と、その項目の総トランザクション、許可トランザクション、ブロック トランザクション、データ使用量、および送受信されたバイト数が表示されます。未処理の [値（Values）] と [パーセンテージ（Percentages）] パーセントの間で数値を切り替え、上位 10、100、または 1000 エントリを表示できます。項目がリンクの場合は、その項目をクリックすると、詳細情報を含む概要ダッシュボードが表示されます。

ステップ 2 コンテンツ テーブルの [ダッシュボード（Dashboard）] リンクをクリックすると、次のデータのダッシュボードが表示されます。

- [ネットワークの概要（Network Overview）]：ネットワークのトラフィックに関する概要情報（一致したアクセス ルール（ポリシー）、トラフィックを開始するユーザ、接続で使用されるアプリケーション、一致した侵入シグネチャ、アクセスされた URL の Web カテゴリ、接続の最も頻繁な宛先など）が表示されます。
- [ユーザ（Users）]：ネットワークの上位ユーザが表示されます。ユーザ情報を表示するには、アイデンティティ ポリシーを設定する必要があります。

- [アプリケーション（Applications）]：ネットワークで使用されている上位アプリケーション（Facebookなど）が表示されます。この情報は、インスペクションが実行された接続についてのみ使用できます。接続は、それらが「許可」ルールや、ゾーン、アドレス、およびポート以外の基準を使用するブロック ルールと一致する場合にインスペクションが実行されます。したがって、インスペクションが必要なルールに一致する前に接続が信頼されるかブロックされる場合は、アプリケーション情報を使用できません。
- [Webカテゴリ（Web Categories）]：アクセスしたWebサイトの分類に基づいて、ネットワークで使用されているWebサイトの上位カテゴリ（ギャンブル、教育機関など）が表示されます。この情報を取得するには、トラフィック一致基準としてWebカテゴリを使用する1つ以上のアクセス コントロール ルールがある必要があります。この情報は、ルールに一致するトラフィック、またはルールに一致するかどうかを判断するためにインスペクションが必要なトラフィックについて使用できます。最初のWebカテゴリ アクセス コントロール ルールの前に照会されるルールに一致する接続のカテゴリ（またはレピュテーション）情報は表示されません。
- [ポリシー（Policies）]：ネットワーク トラフィックと一致した上位のアクセス ルールが表示されます。
- [入力ゾーン（Ingress Zones）]：デバイスに入るトラフィックが通過した上位のセキュリティ ゾーンが表示されます。
- [出力ゾーン（Egress Zones）]：デバイスを出るトラフィックが通過した上位のセキュリティ ゾーンが表示されます。
- [宛先（Destinations）]：ネットワーク トラフィックの上位の宛先が表示されます。
- [攻撃者（Attackers）]：上位の攻撃者（侵入イベントをトリガーする接続の送信元）が表示されます。この情報を表示するには、アクセス ルールで侵入ポリシーを設定する必要があります。
- [ターゲット（Targets）]：侵入イベントの上位のターゲット（攻撃の被害者）が表示されます。この情報を表示するには、アクセス ルールで侵入ポリシーを設定する必要があります。
- [脅威（Threats）]：トリガーされた上位の侵入ルールが表示されます。この情報を表示するには、アクセス ルールで侵入ポリシーを設定する必要があります。
- [ファイル ログ（File Logs）]：ネットワーク トラフィックに見られる上位のファイル タイプが表示されます。この情報を表示するには、アクセス ルールでファイル ポリシーを設定する必要があります。
- [システム（System）]：システムの全体像（インターフェイスとそのステータス（インターフェイスにマウス カーソルを合わせるとIPアドレスが表示される）や全体的なシステム スループットに加え、システム イベント、CPU使用率、メモリ使用率、およびディスク使用率に関する概要情報など）が表示されます。すべてのインターフェイスではなく特定のインターフェイスが表示されるようにスループットのグラフを制限することができます。

（注） システム ダッシュボードに表示される情報は、システム全体のレベルです。デバイスの CLI にログインすると、さまざまなコマンドを使用して詳細情報を表示できます。たとえば、**show cpu** コマンドと **show memory** コマンドには追加の詳細情報を表示するためのパラメータがありますが、これらのダッシュボードには **show cpu system** コマンドと **show memory system** コマンドのデータが表示されます。

ステップ 3 コンテンツ テーブルの次のリンクをクリックすることもできます。

- [イベント（Events）]：発生したイベントが表示されます。これらのルールに関連する接続イベントを表示するには、個々のアクセス ルールで接続ロギングを有効にする必要があります。これらのイベントは、ユーザの接続に関する問題を解決するために役立ちます。

コマンドラインを使用した追加の統計のモニタリング

Firepowerデバイス マネージャのダッシュボードは、デバイスを経由するトラフィックと全般的なシステムの使用状況に関する広範な統計情報を提供します。ただし、デバイス CLI にログインすることで、ダッシュボードでカバーされていない領域の追加情報を取得できます（コマンドライン インターフェイス（CLI）へのログインを参照）。

CLI には、これらの統計情報を提供するためのさまざまな **show** コマンドが含まれています。また、**ping** や **traceroute** などのコマンドを含め、一般的なトラブルシューティングに CLI を使用することもできます。ほとんどの **show** コマンドには統計を 0 にリセットするための **clear** コマンドが付随しています。

コマンドの詳細については、『*Command Reference for Firepower Threat Defense*』（http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html）を参照してください。

たとえば、次のコマンドは全般的に役立つ場合があります。

- **show nat** は、NAT ルールのヒット数を表示します。
- **show xlate** は、アクティブな実際の NAT 変換を表示します。
- **show conn** は、デバイスを経由する現在の接続に関する情報を提供します。
- **show dhcpd** は、インターフェイスに設定している DHCP サーバに関する情報を提供します。
- **show interface** は、各インターフェイスの使用状況の統計情報を提供します。

イベントの表示

ロギングを有効化するアクセス ルールから生成されたイベントを表示できます。また、イベントは、トリガーされた侵入ポリシーとファイル ポリシーから生成されます。

イベント ビューア テーブルには、リアルタイムに生成されたイベントが示されます。新しいイベントが生成されると、古いイベントはテーブルから削除されます。

はじめる前に

特定のタイプのイベントが生成されるかどうかは、関連するポリシーに一致する接続に加えて、次の要素によって決まります。

- 接続イベント：アクセス ルールは、接続ロギングを有効化する必要があります。
- 侵入イベント：アクセス ルールは、侵入ポリシーを適用する必要があります。
- ファイルおよびマルウェア イベント：アクセス ルールは、ファイル ポリシーを適用して、ファイル ロギングを有効化する必要があります。

手順

ステップ 1 メイン メニューの [モニタリング（Monitoring）]をクリックします。

ステップ 2 コンテンツのテーブルから [イベント（Events）]を選択します。
イベント ビューアでは、イベントのタイプに基づいてイベントがタブに分類されます。詳細については、イベント タイプ，（7 ページ）を参照してください。

ステップ 3 表示するイベント タイプのタブをクリックします。
イベント リストでは、次の操作を実行できます。

- イベントをより簡単に検索、分析できるようにするために、新しいイベントの追加を停止するには、[一時停止（Pause）]をクリックします。新しいイベントが表示されるようにするには、[再開（Resume）]をクリックします。
- 新しいイベントが表示される速さを制御するには、別の更新率（5、10、20、または 60 秒）を選択します。
- 必要なカラムを含むカスタム ビューを作成します。カスタム ビューを作成するには、タブバーの [+]ボタンをクリックするか、[カラムの追加/削除（Add/Remove Columns）]をクリックします。事前設定されているタブは変更できないため、カラムを追加または削除すると新しいビューが作成されます。詳細については、カスタム ビューの設定，（8 ページ）を参照してください。
- カラム幅を変更するには、カラム ヘッダーの境界をクリックして、目的の幅までドラッグします。
- イベントに関する詳細情報を表示するには、イベントの上にカーソルを置き、[詳細の表示（View Details）]をクリックします。イベントの各フィールドの説明については、イベント フィールドの説明，（10 ページ）を参照してください。

ステップ 4 必要な場合は、テーブルにフィルタを適用することで、さまざまなイベント属性に基づいて目的のイベントを見つけることができます。
新規フィルタを作成するには、ドロップダウン リストからアトミック要素を選択してフィルタを手動で入力し、フィルタの値を入力するか、フィルタリングの基準となる値を含むイベント テー

ブルのセルをクリックしてフィルタを作成します。同じカラムにある複数のセルをクリックして値の間にOR条件を作成するか、異なるカラムにあるセルをクリックしてカラムの間にAND条件を作成することができます。セルをクリックしてフィルタを作成した場合は、得られたフィルタを編集して、適切に調整することもできます。フィルタの作成ルールの詳細については、イベントのフィルタリング, （9 ページ）を参照してください。

フィルタを作成したら、次の操作を実行します。

- フィルタを適用してテーブルを更新し、フィルタと一致するイベントのみが表示されるようにするには、[フィルタ（Filter）]ボタンをクリックします。
- 適用したフィルタをすべてクリアして、フィルタリングされていない状態のテーブルに戻るには、[フィルタ（Filter）]ボックスの [フィルタのリセット（Reset Filters）] をクリックします。
- フィルタのいずれかのアトミック要素をクリアするには、要素の上にカーソルを置き、要素の [X]をクリックします。[フィルタ（Filter）]ボタンをクリックします。

イベント タイプ

システムでは、以下のタイプのイベントが生成されます。この情報に関連する統計情報をモニタリング ダッシュボードに表示するには、これらのイベントを生成する必要があります。

接続イベント

ユーザが生成するトラフィックがシステムを通過する場合、この接続に対してイベントを生成できます。接続イベントは、アクセス ルールで接続のロギングを有効にしている場合のみに表示できます。

接続イベントには接続に関する幅広い種類の情報が含まれ、これには送信元と宛先のIPアドレスおよびポート、使用されたURLおよびアプリケーション、送信されたバイト数またはパケット数などがあります。この情報には、実行されたアクション（接続の許可またはブロックなど）、接続に適用されたポリシーも含まれます。

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のインスペクションを実行し、ホストとそのデータの可用性、整合性、および機密性に影響を与える可能性がある悪意のあるアクティビティについて調べます。システムは潜在的な侵入を識別すると、侵入イベントを生成します。これには、エクスプロイトの日時とタイプ、攻撃とそのターゲットについての状況説明が記録されます。

ファイル イベント

ファイル イベントは、作成したファイル ポリシーに基づき、ネットワーク トラフィック内でシステムによって検出（オプションとしてブロック）されたファイルを表します。これらのイベントを生成するには、ファイル ポリシーを適用するアクセス ルールに対してファイル ロギングを有効にする必要があります。

システムはファイル イベントを生成する場合、基になったアクセス コントロール ルールのロギング設定にかかわらず、関連する接続の終了についても記録します。

マルウェア イベント

ネットワーク トラフィック内のマルウェア検出は、全体的なアクセス コントロール設定の一環として行われます。AMP for Firepower は、結果として生じたイベントの性質や、いつどこでどのようにしてマルウェアが検出されたかに関するコンテキスト データを含むマルウェア イベントを生成できます。これらのイベントを生成するには、ファイル ポリシーを適用するアクセス ルールに対してファイル ロギングを有効にする必要があります。

カスタム ビューの設定

独自のカスタム ビューを作成して、イベントを表示すると目的のカラムが簡単に表示されるようにできます。また、事前定義ビューは編集または削除できませんが、カスタム ビューは編集または削除できます。

手順

ステップ 1 [モニタリング（Monitoring）] > [イベント（Events）] を選択します。

ステップ 2 次のいずれかを実行します。

- 既存のカスタム（または定義された）ビューに基づいて新規ビューを作成するには、そのビューのタブをクリックしてから、タブの左側にある [+]ボタンをクリックします。
- 既存のカスタム ビューを編集するには、そのビューのタブをクリックします。

（注） カスタム ビューを削除するには、ビューのタブにある [X]ボタンをクリックします。削除すると、元に戻すことはできません。

ステップ 3 右側のイベント テーブルの上にある [カラムの追加または削除（Add/Remove Columns）]リンクをクリックし、選択したリストに、ビューに含めるカラムのみが含まれるようになるまで、カラムを選択または選択解除します。
使用可能な（ただし使用されていない）リストと選択されているリストの間で、カラムをクリックしてドラッグします。選択されているリスト内でカラムをクリックしてドラッグし、左から右に向かうテーブル内でのカラムの順番を変更することもできます。カラムについては、イベント フィールドの説明, （10 ページ）を参照してください。

完了したら [OK]をクリックして、カラムの変更を保存します。

（注） 事前定義されたビューを表示しながらカラムの選択を変更すると、新規ビューが作成されます。

ステップ 4 必要に応じてカラムのセパレータをクリックしてドラッグし、カラムの幅を変更します。

イベントのフィルタリング

現在関心のあるイベントだけが表示されるように、複合的なフィルタを作成して、イベント テーブルの表示を制限できます。フィルタの作成には、以下の手法を単独で、またはいくつかを組み合わせて使用できます。

列のクリック

最も簡単なフィルタ作成方法は、イベント テーブル内で、フィルタ処理の基準に使用したい値を持つセルをクリックすることです。セルをクリックすると、[フィルタ（Filter）]フィールドが更新され、この値とフィールドの組み合わせに対して適切に作成されたルールが入力されます。ただし、この手法は、既存のイベント リストに必要な値が含まれていることが前提となります。

すべての列をフィルタ処理することはできません。フィルタ処理可能なデータが含まれるセルでは、このセルにマウス オーバーすると、セルに下線が表示されます。

アトミック要素の選択

もう1つのフィルタ作成方法は、[フィルタ（Filter）]フィールド内をクリックして、ドロップダウン リストから必要なアトミック要素を選択し、一致する値を入力する方法です。これらの要素には、イベント テーブル内の列としては表示されないイベント フィールドが含まれます。また、入力した値と表示するイベントとの関係を定義するための演算子も含まれます。列をクリックする場合は、常に「等号（=）」フィルタとなりますが、要素を選択する場合は、数値フィールドに対して「より大きい（>）」または「より小さい（<）」も選択できます。

どのような方法で要素を[フィルタ（Filter）]フィールドに追加する場合でも、フィールドに直接入力して、演算子や値を調整できます。[フィルタ（Filter）]をクリックすると、テーブルにフィルタが適用されます。

イベント フィルタの演算子

イベント フィルタには、以下の演算子を使用できます。

=	次の値と等しい。イベントは指定の値と一致します。ワイルドカードを使用することはできません。
!=	次の値と等しくない。イベントは指定の値と一致しません。不等号による式を作成するには、「!（感嘆符）」を入力する必要があります。

>	次の値より大きい。イベントに、指定の値より大きな値が含まれます。この演算子は、ポートや IP アドレスなど、数値のみに使用できます。
<	次の値より小さい。イベントに、指定の値より小さな値が含まれます。この演算子は数値のみに使用できます。

複合イベント フィルタのルール

複数のアトミック要素を保持する複合フィルタを作成する場合は、以下のルールに注意します。

- 同じタイプの要素は、このタイプのすべての値が互いに「論理和（OR）」の関係となります。たとえば、イニシエータ IP = 10.100.10.10 とイニシエータ IP = 10.100.10.11 を含めると、このどちらかのアドレスがトラフィック送信元となるイベントが適合します。
- 異なるタイプの要素は、「論理積（AND）」の関係となります。たとえば、イニシエータ IP = 10.100.10.10 と宛先ポート/ICMP タイプ= 80 を含めると、この発信元アドレスを持ち、かつこの宛先ポートを持つイベントのみが適合します。10.100.10.10 から別の宛先ポートに向かうイベントは、表示されません。
- IPv4 および IPv6 アドレスなど、数値要素は範囲を指定できます。たとえば、宛先ポート = 50-80 と指定すると、この範囲内のポートに送信されるすべてのトラフィックがキャプチャされます。範囲の開始値と終了値は、ハイフンでつなぎます。すべての数値フィールドで範囲を指定できるわけではありません。たとえば、送信元要素には、IP アドレス範囲を指定することはできません。
- ワイルドカード、または正規表現は使用できません。

イベント フィールドの説明

ここでは、各イベントに含めることのできる情報について説明します。この情報を読むには、イベントの詳細を表示します。また、関心の高い情報を表示する列をイベント ビューア テーブルに追加することもできます。

以下に、使用可能なフィールドの一覧を示します。すべてのイベント タイプに対し、すべてのフィールドが適用されるわけではありません。それぞれのイベントで使用可能な情報は、システムが接続を記録する方法、理由、およびタイミングによって異なることに注意してください。

アクション（Action）

接続イベントにおいて、接続を記録したアクション コントロール ルールに関連付けられたアクション、またはデフォルト アクション。

許可（Allow）

明示的に許可された接続。

信頼（Trust）

信頼できる接続。信頼ルールによって最初のパケットで検出されたTCP接続は、接続終了イベントだけを生成します。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）

ブロックされた接続。以下の条件下で、ブロック（Block）アクションを許可（Allow）アクセス ルールに関連付けることができます。

- 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。

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状況。

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付けられた、ビジネスとの関連性。「非常に高い（Very High）」、「高（High）」、「中（Medium）」、「低（Low）」、「非常に低い（Very Low）」のいずれかとなります。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 タグ（Application Tag）

アプリケーションの機能を分かりやすくするため、アプリケーションの特徴付けに使用される基準。

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付けられたリスク。「非常に高い（Very High）」、「高（High）」、「中（Medium）」、「低（Low）」、「非常に低い（Very Low）」のいずれかとなります。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。

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 アプリケーション（Client Application）、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 アプリケーションおよびクライアント バージョン。

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付けられた、ビジネスとの関連性。「非常に高い（Very High）」、「高（High）」、「中（Medium）」、「低（Low）」、「非常に低い（Very Low）」のいずれかとなります。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 Category）、クライアント タグ（Client Tag）

アプリケーションの機能を分かりやすくするため、アプリケーションの特徴付けに使用される基準。

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付けられたリスク。「非常に高い（Very High）」、「高（High）」、「中（Medium）」、「低（Low）」、「非常に低い（Very Low）」のいずれかとなります。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。

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。

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）

受信ホストの IP アドレス。

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

セッション レスポンダによって使用されるポートまたは ICMP コード。

方向（Direction）

ファイルの送信方向。

傾向（Disposition）

ファイルの傾向。

マルウェア（Malware）

AMP クラウドによってファイルがマルウェアと分類されたか、またはファイルの脅威スコアがファイル ポリシーに定義されたマルウェアのしきい値を超えたこと示します。

正常（Clean）

AMP クラウドによってファイルが正常であると分類されたことを示します。

不明（Unknown）

システムが AMP クラウドに問い合わせたが、ファイルに傾向が割り当てられていなかった（このファイルが AMP クラウドによって分類されていない）ことを意味します。

使用不可（Unavailable）

システムによる AMP クラウドへの照会が失敗したことを示します。この性質に関するイベントが、わずかながら存在する可能性があります。これは予期された動作です。

該当なし

ファイル検出（Detect Files）ルールまたはファイル ブロック（Block Files）ルールによってこのファイルが処理され、AMP クラウドへの照会は行われませんでした。

出力インターフェイス（Egress Interface）、出力セキュリティ ゾーン（Egress Security Zone）

接続がデバイスを通過する出口となるインターフェイスおよびゾーン。

イベント（Event）、イベント タイプ（Event Type）

イベントのタイプ。

イベントの秒数（Event Seconds）、イベントのマイクロ秒数（Event Microseconds）

イベントの検出時を表す秒単位またはマイクロ秒単位の値。

ファイル カテゴリ（File Category）

ファイル タイプの一般分類。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）

ファイルの名前。

ファイル ルール アクション（File Rule Action）

ファイルを検出したファイル ポリシー ルールに関連付けられたアクション、および関連するすべてのファイル ルール アクション オプション。

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（KB）（File Size）

キロバイト単位のファイル サイズ。受信が完了する前にシステムによってブロックされたファイルの場合、ファイル サイズが空になることがあります。

ファイル タイプ（File Type）

ファイルの種類（HTML、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（Firewall Policy Rule）、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。

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）。

HTTP 応答（HTTP Response）

クライアントの HTTP 要求への応答として、接続上を送信された HTTP ステータス コード。

IDS の分類（IDS Classification）

イベントを生成したルールが属する分類。

入力インターフェイス（Ingress Interface）、入力セキュリティ ゾーン（Ingress Security Zone）

接続がデバイスを通過する入口となるインターフェイスおよびゾーン。

イニシエータのバイト数またはパケット数（Initiator Bytes, Initiator Packets）

セッション イニシエータが送信したバイト数またはパケット数の合計。

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

セッションを開始したホストが属する国または大陸。イニシエータのIPアドレスがルーティング可能である場合にのみ使用可能です。

イニシエータ IP（Initiator IP）

セッションを開始したホストのIPアドレス（DNS解決が有効化されている場合はIPアドレスおよびホスト名）。

インライン結果（Inline Result）

侵入イベントを トリガーさせたパケットが実際に破棄されたか、または、もしインラインモードで動作していたとしたら破棄されていたかどうか。空白の場合は、トリガーされたルールが「破棄およびイベント生成（Drop and Generate Events）」に設定されていなかったことを意味します。

侵入ポリシー（Intrusion Policy）

イベントを生成させたルールが有効化された侵入ポリシー。

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）

侵入イベントの場合は、このイベントを説明するテキスト。マルウェアまたはファイル イベントの場合は、マルウェア イベントに関連付けられた何らかの補足情報。

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または大陸（Original Client Country and Continent）

セッションを開始した元のクライアント ホストが属する国または大陸。元のクライアントの IP アドレスがルーティング可能である場合にのみ使用可能です。

元のクライアント IP（Original Client IP）

HTTP接続を開始した元のクライアントIPアドレス。このアドレスはX-Forwarded-For（XFF）または True-Client-IP HTTP ヘッダー フィールド、またはこの同等フィールドから取得されます。

ポリシー（Policy）、ポリシー リビジョン（Policy Revision）

イベントに関連付けられたアクセス（ファイアウォール）ルールが含まれるアクセス コントロール ルールとそのリビジョン。

優先順位（Priority）

Cisco Talos Security Intelligence and Research Group（Talos）によって決定されたイベントの優先順位。「高（high）」、「中（medium）」、「低（low）」のいずれかとなります。

プロトコル（Protocol）

接続に使用されるトランスポート プロトコル。

理由（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。

理由	説明
ファイル ブロック（File Block）	接続に、システムが送信を阻止するファイルまたはマルウェア ファイルが含まれます。理由「ファイル ブロック」は、常に「ブロック」アクションとペアになります。
ファイルモニタ（File Monitor）	接続内に特定のファイル タイプが検出されました。
ファイルの再開を許可（File Resume Allow）	最初に、「ファイルまたはマルウェア ファイルのブロック」ルールによってファイル伝送がブロックされました。このファイルを許可するアクセス コントロール ポリシーが新たに展開された後、HTTP セッションが自動的に再開されました。
ファイルの再開をブロック（File Resume Block）	最初に、「ファイルまたはマルウェア クラウド ルックアップ ファイルの検出」ルールによってファイル伝送が許可されました。このファイルをブロックするアクセス コントロール ポリシーが新たに展開された後、HTTP セッションが自動的に停止されました。
侵入ブロック（Intrusion Block）	接続中に検出されたエクスプロイト（侵入ポリシー違反）が実際にブロックされたか、またはブロックされていたことが想定されるか。理由「侵入ブロック」は、エクスプロイトがブロックされた場合は「ブロック」、ブロックされていたことが想定される場合は「許可」アクションとペアになります。
侵入モニタ（Intrusion Monitor）	接続中のエクスプロイトが検出されましたが、ブロックされませんでした。これは、トリガーされた侵入ルールの状態が「イベントの生成（Generate Events）」である場合です。

受信時間（Receive Times）

イベントが生成された日時。

参照ホスト（Referenced Host）

接続に使用されたプロトコルが HTTP または HTTPS であれば、このフィールドには、それぞれのプロトコルが使用したホストの名前が表示されます。

レスポンダのバイト数またはパケット数（Responder Bytes、Responder Packets）

セッション レスポンダが送信したバイト数またはパケット数の合計。

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

セッションに応答したホストが属する国または大陸。レスポンダの IP アドレスがルーティング可能である場合にのみ使用可能です。

レスポンダ IP（Responder IP）

セッション レスポンダのホスト IP アドレス（DNS 解決が有効化されている場合は IP アドレスおよびホスト名）。

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。送信元 IP アドレスがルーティング可能である場合にのみ使用可能です。

送信元 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。

送信元のポート/ICMP タイプ（Source Port/ICMP Type）、送信元ポート（Source Port）、送信元ポート Itype（Source Port Itype）

セッション イニシエータに使用されるポートまたは ICMP タイプ。

TCP フラグ（TCP Flags）

接続で検出された TCP フラグ。

URL、URL カテゴリ（URL Category）、URL レピュテーション（URL Reputation）、URL レピュテーション スコア（URL Reputation Score）

セッション中、モニタリングされているホストから要求された URL と、これに関連するカテゴリ、レピュテーション、レピュテーション スコア（ある場合）。

SSL アプリケーションが識別またはブロックされた場合は、要求された URL は暗号化トラフィックであり、このトラフィックは SSL 証明書に基づいて識別されます。したがって、SSL アプリケーションの場合は、URL は証明書内の共通名を表しています。

ユーザ（User）

イニシエータ IP アドレスに関連付けられたユーザ。

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付けられた、ビジネスとの関連性。「非常に高い（Very High）」、「高（High）」、「中（Medium）」、「低（Low）」、「非常に低い（Very Low）」のいずれかとなります。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およびタグ（Web App Categories、Web App Tag）

Web アプリケーションの機能を分かりやすくするため、Web アプリケーションの特徴付けに使用される基準。

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付けられたリスク。「非常に高い（Very High）」、「高（High）」、「中（Medium）」、「低（Low）」、「非常に低い（Very Low）」のいずれかとなります。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（Web Application）

接続で検出された HTTP トラフィックに対応する、コンテンツまたは要求 URL を表す Web アプリケーション。

このイベントの URL に Web アプリケーションが一致しない場合は、このトラフィックは参照先トラフィック（広告トラフィックなど）を表していることが考えられます。参照先トラフィックが検出された場合は、参照元アプリケーション（存在する場合）が保管され、このアプリケーションが Web アプリケーションとしてリストされます。