デバイスのモニタリング

システムには、デバイスと、デバイスを通過するトラフィックを監視するために使用できるイベント ビューアとダッシュボードがあります。

トラフィック統計を取得するためのロギングの有効化

監視ダッシュボードとイベント ビューアを使用して、広範囲に及ぶトラフィック統計をモニタすることができます。ただし、どの統計情報を収集すべきかシステムに知らせるためにロギングを有効にする必要があります。ロギングでは、システムを通過する接続に対して有用な情報を提供するさまざまな種類のイベントを生成します。

ここでは、イベントと提供される情報について、特に接続ロギングに重点を置いて詳しく説明します。

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。監視ダッシュボードで関連する統計を表示するには、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

ユーザがシステムを通過するトラフィックを生成すると、その接続に関するイベントが生成されます。これらのイベントを生成するには、アクセス ルールで接続ロギングを有効にします。また、セキュリティ インテリジェンス ポリシーおよび SSL 復号ルールでロギングを有効にすると、接続イベントを生成できます。

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。情報には、実行されたアクション（接続の許可やブロックなど）や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、ホストとそのデータの可用性、整合性、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。侵入イベントは、アクセス制御ルールのロギング設定に関係なく、ブロックまたはアラートするように設定された侵入ルールに対して生成されます。

ファイル イベント

ファイル イベントは、ファイル ポリシーに基づいてシステムがネットワーク トラフィック内でファイルを検出して、必要に応じてブロックしたことを表します。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 ルールでファイル 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 イベントの生成時に、アクセス制御ルールのロギング設定に関係なく、接続終了時の情報もロギングします。

マルウェア イベント

システムは、全体的なアクセス コントロール設定の一環として、ネットワーク トラフィックのマルウェアを検出できます。malware defense 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。

ファイルの判定結果は、正常からマルウェア、マルウェアから正常などに変更できます。malware defense が Secure Malware Analytics Cloudにファイルについて照会し、クエリから 1 週間以内に判定結果が変更されたことがクラウドに特定されると、システムはレトロスペクティブ マルウェア イベントを生成します。

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 イベントは、ポリシーによってブロックまたはモニタされた各接続の、セキュリティ インテリジェンス ポリシーによって生成された接続イベントの一種です。すべてのセキュリティ インテリジェンス イベントには、自動入力された [セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）] フィールドがあります。

これらのイベントのそれぞれについて、対応する「通常」の接続イベントがあります。セキュリティインテリジェンスポリシーはアクセスコントロールなどのその他多数のセキュリティ ポリシーより前に評価されるため、セキュリティ インテリジェンスによって接続がブロックされると、その結果のイベントには、以降の評価から収集される情報（ユーザアイデンティティなど）は含まれません。

設定可能な接続ロギング

組織のセキュリティとコンプライアンスのニーズに応じて、接続をログに記録する必要があります。生成されるイベントの数を抑えてパフォーマンスを向上させることを目標にする場合は、分析のために重要な意味を持つ接続のロギングだけを有効化してください。ただし、プロファイリングのためにネットワークトラフィックを広範囲に把握したい場合は、他の接続のロギングを追加で有効にできます。

システムは複数の理由で接続をログできるため、1 つの場所でログを無効にしても、一致する接続がログされないとは限りません。

接続ロギングは次の場所で設定できます。

- アクセス制御ルールおよびデフォルトアクション：接続終了時点のロギングは、接続に関するほとんどの情報を提供します。接続の開始も記録できますが、これらのイベントの情報は不完全です。接続ロギングはデフォルトで無効になっているため、追跡するトラフィックを対象としたルール（およびデフォルトアクション）ごとにこのロギングを有効にする必要があります。
- セキュリティ インテリジェンス ポリシー：ブロックされた接続ごとにセキュリティ インテリジェンス接続イベントを生成するようにロギングを有効にすることができます。セキュリティ インテリジェンス フィルタリングの結果として接続イベントがロギングされる場合、一致するセキュリティインテリジェンスイベントもロギングされます。これは、別々に表示および分析できる特殊な接続イベントです。
- SSL 復号ルールとデフォルトのアクション：接続の最後にロギングを設定できます。ブロックされた接続では、システムはすぐにセッションを終了し、イベントを生成します。モニタ対象の接続とアクセス制御ルールに渡す接続では、セッションが終了する際にイベントが生成されます。

自動接続ロギング

他のロギング設定に関係なく、次の接続終了イベントは自動的に保存されます。

- システムは、接続がアクセス コントロール ポリシーのデフォルトのアクションで処理される限り、侵入イベントに関連付けられている接続を自動的に記録します。一致するトラフィックの侵入イベントを取得するには、デフォルトアクションでロギングを有効に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に関連付けられている接続は自動的に記録されます。（接続イベントのみ）：必要に応じてファイルおよびマルウェアイベントの生成を無効にできます。

接続ロギングのためのヒント

ロギング設定および関連する統計情報の評価を検討する際は、次のヒントに注目してください。

- アクセス制御ルールを使ってトラフィックを許可する場合、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検査し、最終目的地に到達する前に、侵入や禁止ファイル、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、暗号化されたペイロードに対するファイルインスペクションと侵入インスペクションはデフォルトで無効になっていることに注意してください。侵入ポリシーまたはファイルポリシーで接続をブロックする理由が特定された場合は、接続ログ設定に関係なく、システムが速やかに接続終了イベントを記録します。許可された接続のロギングは、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提供します。
- 信頼された接続とは、信頼アクセス制御ルールまたはアクセス制御ポリシー内のデフォルトアクションによって処理された接続です。ただし、信頼された接続では、ディスカバリデータ、侵入、禁止ファイルとマルウェアの検査は行われません。したがって、信頼された接続の接続イベントに含まれている情報には限りがあります。
- トラフィックをブロックするアクセス制御ルールとアクセス制御ポリシー のデフォルトアクションにおいては、システムが接続開始イベントをロギングします。一致するトラフィックは、さらに検査されることなく拒否されます。
- サービス妨害（DoS）攻撃中にブロックされたTCP接続のロギングは、複数の同様のイベントでシステムのパフォーマンスに影響を与え、データベースのパフォーマンス低下させる可能性があります。ブロック ルールのロギングを有効にする際は、そのルールでモニタするトラフィックが、インターネット側のインターフェイス上なのか、DoS攻撃に脆弱なその他のインターフェイス上なのかを確認してください。
- リモート アクセス VPN接続プロファイルの設定時に、[復号されたトラフィックでアクセスコントロールポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] オプションを選択した場合、または **sysopt connection permit-vpn** コマンドをイネーブルにした場合は、すべてのサイト間またはリモート アクセス VPN トラフィックがインスペクションとアクセス コントロール ポリシーをバイパスします。したがって、このトラフィックに対する接続イベントは発生せず、トラフィックは統計ダッシュボードには反映されません。

外部の Syslog サーバへのイベントの送信

イベントを格納する容量が限られている、Device Manager を通してイベントを表示する以外に、外部の Syslog サーバーにイベントを送信するルールとポリシーを設定することもできます。この機能と、選択した syslog サーバ プラットフォームの追加のストレージを使用して、イベント データを表示および分析できます。

外部のsyslogサーバにイベントを送信するには、各ルール、デフォルトのアクション、または接続のログ記録を有効にするポリシーを編集し、ログ設定のsyslogサーバオブジェクトを選択します。侵入イベントをsyslogサーバに送信するには、侵入ポリシーの設定でサーバを設定します。Syslog サーバにファイル/マルウェア イベントを送信するには、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[ロギング設定（Logging Settings）]** でサーバを設定します。

詳細については、各ルールとポリシーの種類に応じたヘルプおよびsyslog サーバの設定を参照してください。

Cisco Cloud ベースのサービスを使用したイベントの評価

イベント ビューアと独自の syslog サーバーを使用することに加えて、接続イベントおよび高プライオリティの侵入/ファイル/マルウェア関連イベントをシスコのクラウドベース サーバーに送信できます。Threat Response など、シスコのクラウドベースのサービスでは、クラウド サーバーからイベントをプルし、各サービスを使用してそれぞれのイベントを評価できます。

これらのクラウドベースのサービスは、脅威に対する防御 デバイスと Device Manager で分離されています。イベントを Cisco Cloud に送信する必要があるサービスを使用することを選択する場合は、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[クラウドサービス（Cloud Services）]** ページで接続を有効にする必要があります。「Cisco Cloud へのイベントの送信」を参照してください。

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

システムにはいくつかのダッシュボードが含まれており、デバイスを通過するトラフィックやセキュリティ ポリシーの結果の分析に使用できます。ダッシュボード情報は、構成全体の有効性を評価し、ネットワークの問題を特定して解決するために使用します。

高可用性グループ内の装置のダッシュボードには、そのデバイスの統計情報のみ表示されます。統計情報は装置間で同期されません。

（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 ロギングを有効にするアクセス制御ルール、およびロギングを許可するその他のセキュリティ ポリシーから収集されます。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と一致するトラフィックは反映されません。問題に関連する重要な情報を記録するルールが設定されていることを確認します。ユーザ情報は、ユーザ アイデンティティを収集するアイデンティティ ルールが設定されてい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 URL カテゴリの情報を使用できます。ただし、これを使用できるのは、これらの機能に関するライセンスを所有しており、機能を使用するルールを設定している場合のみです。

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。

ダッシュボードのグラフおよびテーブルに表示されているデータを制御するには、事前定義された時間範囲（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を指定してカスタムの時間範囲を定義することができます。

トラフィック関連のダッシュボードには、次のタイプのディスプレイがあります。

- [上位 5 つの棒グラフ（Top 5 bar graphs）]：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、項目ごとのサマリー ダッシュボードには、ダッシュボード テーブルで特定のアイテムをクリックしたかどうかが表示されます。[トランザクション（Transactions）] または [データ使用（Data Usage）]（送受信バイト数の合計）のカウント間で情報を切り替えることができます。さらに、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。グラフと関連付けられている表を確認する場合は、[追加表示（View More）] をクリックします。
- [テーブル（Tables）]：テーブルには、特定のタイプの項目（アプリケーションまたはURL カテゴリなど）およびその項目の合計トランザクション数、許可トランザクション数、ブロック トランザクション数、データ使用量、および送受信バイト数が表示されます。未加工の [値（Values）] と [パーセンテージ（Percentages）] 間の数字は切り替えることができ、上位 10、100、または 1000 エントリが表示されます。項目がリンクの場合は、そのリンクをクリックしてサマリー ダッシュボードとその詳細情報を表示できます。

ステップ 2 目次にある [ダッシュボード（Dashboard）] リンクをクリックして、次のデータのダッシュボードを表示します。

- [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サマリー情報を表示します。これには、一致したアクセス ルール（ポリシー）、トラフィックを開始したユーザ、接続で使用されたアプリケーション、一致した侵入シグネチャ、アクセスされた URL の URL カテゴリ、および最も頻繁に接続される宛先が含まれます。
- [ユーザ（Users）]：ネットワークの上位ユーザを示します。ユーザ情報を表示するには、IDポリシーを設定する必要があります。ユーザアイデンティティがない場合は、送信元IP アドレスが含まれます。以下の特殊なエンティティが表示される場合があります。
  - [認証失敗（Failed Authentication）]：ユーザが認証を求められ、有効なユーザ名/パスワードを入力できずに最大試行回数に達しました。認証の失敗により、ユーザがネットワークにアクセスできなくなることはありませんが、このようなユーザに対してネットワーク アクセスを制限するアクセス ルールを作成できます。
  - [ゲスト（Guest）]：ゲスト ユーザは [認証失敗（Failed Authentication）] ユーザと似ていますが、アイデンティティ ルールでこのようなユーザがゲストと呼ばれるように設定されている点で異なります。ゲスト ユーザが認証を求められましたが、認証できずに最大試行回数に達しました。
  - [認証不要（No Authentication Required）]：ユーザの接続が、認証不要と指定されているアイデンティティ ルールに一致したため、ユーザは認証を求められませんでした。

- [不明（Unknown）]：IPアドレスのユーザマッピングがないため、認証失敗の記録がありません。通常、これは、HTTP トラフィックがそのアドレスからまだ見られてないことを意味します。

- [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（HTTPなど）を示します。この情報は、インスペクションを実行済みの接続にのみ提供されます。接続にインスペクションが行われるのは、「許可」ルールと一致した場合、および、ゾーン、アドレス、およびポート以外の条件を使用するブロックルールと一致した場合です。そのため、インスペクションが必要なルールにヒットする前に接続が信頼またはブロックされている場合、アプリケーション情報は使用できません。
- [Webアプリケーション（Web Applications）]：ネットワークで使用されている上位Webアプリケーション（Googleなど）を示します。 Webアプリケーション情報を収集するための条件は、アプリケーション ダッシュボードの場合と同じです。
- **[URLカテゴリ（URL Categories）]**：参照するWebサイトのカテゴリに基づいて、ネットワークで使用されているWebサイトのカテゴリ（ギャンブルや教育機関など）を示します。この情報を入手するには、トラフィック一致基準としてURLカテゴリを使用する少なくとも1つのアクセス制御ルールが存在する必要があります。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を実行する必要があるトラフィックに関してのみ提供されます。最初のWebカテゴリのアクセス コントロール ルールよりも前にあるルールと一致する接続に関するカテゴリ（またはレピュテーション）情報は表示されません。
- [アクセスおよびSIルール（Access And SI Rules）]：ネットワーク トラフィックで一致した上位アクセス ルールおよびセキュリティ インテリジェンス ルールに相当するものを示します。
- [ゾーン（Zones）]：デバイスに入ってから出ていくトラフィックの上位セキュリティゾーンのペアを示します。
- [宛先（Destinations）]：ネットワーク トラフィックの宛先を示します。
- [攻撃者（Attackers）]：侵入イベントをトリガーする接続の送信元である、上位の攻撃者を示します。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）]：攻撃の犠牲者である、侵入イベントの上位ターゲットを示します。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を示します。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 トラフィックに表示される上位のファイル タイプを示します。この情報を表示するには、アクセス ルールにファイル ポリシーを設定する必要があります。
- [マルウェア（Malware）]：上位マルウェアのアクションとディスポジションの組み合わせを示します。 ドリルダウンして関連付けられているファイル タイプの情報を参照できま

す。この情報を表示するには、アクセス ルールにファイル ポリシーを設定する必要があります。

- 可能なアクション：マルウェア クラウドルックアップ、ブロック、アーカイブブロック（暗号化）、検出、カスタム検出、クラウドルックアップのタイムアウト、マルウェアブロック、アーカイブブロック（深さ超過）、カスタム検出ブロック、TIDブロック、アーカイブブロック（検査失敗）。
- 可能なディスポジション：マルウェア、不明、クリーン、カスタム検出、使用不可。

- [SSL復号（SSL Decryption）]：デバイスを経由した暗号化トラフィックとプレーンテキスト トラフィックの内訳、およびSSL 復号ルールに従った暗号化トラフィックの復号方法の内訳を示します。
- [システム（System）]：インターフェイスとそのステータス（マウスをインターフェイスに合わせるとIP アドレスが表示される）、全体的なシステムの平均スループット（最大1 時間で5 分間のバケット、より長い期間で1 時間のバケット）、およびシステム イベント、CPU使用率、メモリ使用率、ディスク使用率に関する概要情報の表示を含む、システムの全体図を示します。 また、スループット グラフは、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に限定して表示できます。

（注）
[システム（System）]ダッシュボードに表示される情報は、全体的なシステム レベルの情報です。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確認できます。たとえば、**show cpu** および **show memory** コマンドには、他の詳細を示すパラメータが含まれますが、これらのダッシュボードには **show cpu system** および **show memory system** コマンドからのデータが表示されます。

ステップ3 目次でこれらのリンクをクリックすることもできます。

- [イベント（Events）]：発生したイベントを表示します。個々のアクセス ルールに関連する接続イベントを表示するには、それぞれのアクセスルールで接続のロギングを有効にする必要があります。また、セキュリティ インテリジェンス ポリシーおよびSSL 復号ルールでロギングを有効にして、セキュリティ インテリジェンス イベントおよびその他の接続イベントデータを参照します。これらのイベントは、ユーザの接続の問題の解決に有効です。
- [セッション（Sessions）]：Device Manager ユーザーセッションを表示および管理します。詳細については、「Device Manager ユーザーセッションの管理」を参照してください。

コマンドラインを使用した追加統計情報のモニタリング

Device Manager ダッシュボードには、デバイスを介して移動するトラフィックや一般的なシステム使用状況に関連するさまざまな統計情報が表示されます。ダッシュボードが対応していな

い領域に関する追加情報は、CLI コンソールを使用するか、またはデバイス CLI にログインすることで得られます（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にはこうした統計情報を提供するためのさまざまな**show**コマンドが含まれます。CLIは一般的なトラブルシューティングにも使用することが可能で、**ping**および**traceroute**といったコマンドが含まれます。ほとんどの**show**コマンドには、統計情報を0にリセットする**clear**コマンドがあります（CLI コンソールから統計情報をクリアすることはできません）。

コマンドのドキュメントは、Cisco Firepower Threat Defense コマンド リファレンス、http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.htmlにあります。

たとえば、次のコマンドが役に立ちます。

- **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で設定した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

ロギングを有効にしたセキュリティ ポリシーによって生成される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 ビューアのテーブルには、生成されるイベントがリアルタイムで表示されます。新しいイベントが生成されるごとに、古いイベントが徐々にテーブルから削除されます。

始める前に

特定のタイプのイベントが生成されるかどうかは、関連するポリシーと一致する条件に加えて、次の内容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。また、セキュリティ インテリジェンス ポリシーおよび SSL 復号ルールで接続ロギングを有効にすることもできます。
- 侵入イベント：アクセス ルールで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 ルールでファイル ポリシーを適用し、ファイル ロギングを有効にする必要があります。
- 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 ポリシーを有効にして設定し、ロギングを有効にする必要があります。

手順

ステップ 1 メイン メニューで [監視（Monitoring）] をクリックします。

ステップ 2 目次から [イベント（Events）] を選択します。

イベント ビューアでは、イベントがタイプごとにタブで表示されます。詳細については、イベント タイプ （1 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行えます。

- [一時停止（Pause）]をクリックして、新しいイベントが追加されるのを停止し、イベントを注意深く分析する。[復帰（Resume）]をクリックして、新しいイベントの表示を再開する。
- 新しいイベントが表示される頻度を更新率（5、10、20、または 60 秒）で選択する。
- 目的の列が含まれるカスタム ビューを作成する。カスタム ビューを作成するには、タブバーにある [+] ボタンをクリックするか、[列の追加/削除（Add/Remove Columns）] をクリックします。事前定義されたタブは変更できないため、列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 （11 ページ）を参照してください。
- カラム幅を変更する。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。
- イベントの上にマウスを置いて [詳細を表示（View Details）] ボタンをクリックし、イベントの完全な情報を表示する。イベント内のさまざまな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 （13 ページ）を参照してください。

ステップ 4 必要に応じて、さまざまなイベント属性に基づいたフィルタをテーブルに適用することで、イベントを検索することができます。

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からその値を入力するか、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、それらの値に 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、さら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 （12 ページ）を参照してください。

フィルタを作成したら、次のいずれかを実行します。

- 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、フィルタなしの状態にテーブルを戻すには、[フィルタ（Filter）] ボックスにある [フィルタのリセット（Reset Filters）] ボタンをクリックします。
- 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、クリアする要素の上にカーソルを置き、[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。

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際、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）]** の順に選択します。

ステップ 2 次のいずれかを実行します。

- 既存のカスタム（または事前定義された）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/削除（Add/Remove Columns）] リンクをクリックし、カラムを選択または選択解除して、ビューに含めるカラムのみが選択リストに含まれるようにします。

使用可能な（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、テーブル内でのカラムの順番（左から右に向かう）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 （13 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

複雑なフィルタを作成してイベントテーブルを制限し、現在関心のあるイベントのみが表示されるようにできます。次の手法を単独または組み合わせて使用して、フィルタを作成できます。

カラムをクリック

フィルタを作成する最も簡単な方法は、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することです。セルをクリックすると、その値とフィールドの組み合わせに正しく定式化されているルールを使用して、[フィルタ（Filter）]フィールドが更新されます。ただし、この手法を使用するには、イベントの既存のリストに目的の値が含まれている必要があります。

すべてのカラムをフィルタリングすることはできません。セルのコンテンツをフィルタリングできる場合は、そのセルの上にカーソルを合わせたときに下線が表示されます。

アトミック要素の選択

[フィルタ（Filter）] フィールドをクリックして、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た後、照合値を入力することでフィルタを作成することもできます。これらの要素には、イベント テーブル内のカラムとして表示されないイベント フィールドが含まれます。また、表示するイベントと入力された値との関係を定義する演算子が含まれます。カラムをクリックすると必ず、「equals (=)」フィルタが表示されますが、要素を選択すると、数値フィールドに「greater than (>)」または「less than (<)」も選択できるようになります。

[フィルタ（Filter）]フィールドに要素を追加する方法に関係なく、フィールドに演算子または値を入力して調整できます。[フィルタ（Filter）]をクリックしてフィルタをテーブルに適用します。

イベント フィルタの演算子

イベント フィルタには、次の演算子を使用できます。

=	等しい。イベントは指定した値と一致します。ワイルドカードを使用することはできません。
!=	等しくない。イベントは指定した値と一致しません。「等しくない」の式を作成するには、感嘆符（!）を入力する必要があります。
>	大なり。イベントに、指定された値よりも大きい値が含まれています。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。
<	小なり。イベントに、指定した値よりも小さい値が含まれます。この演算子は、数値のみに使用できます。

複雑なイベント フィルタのルール

複数のアトミック要素を含む複雑なフィルタを作成する場合、次のルールに注意してください。

- 同じタイプの要素には、そのタイプのすべての値の間に OR 関係があります。たとえば、Initiator IP=10.100.10.10 と Initiator IP=10.100.10.11 を含めると、トラフィックの送信元としてこれらのアドレスのいずれかを含むイベントが一致します。
- 異なるタイプの要素には、AND 関係があります。たとえば、Initiator IP=10.100.10.10 と Destination Port/ICMP Type=80 を含めると、この送信元アドレスと宛先ポートのみを含むイベントが一致します。10.100.10.10 から異なる宛先ポートへのイベントは表示されません。
- IPv4 アドレスや IPv6 アドレスなどの数値要素は範囲を指定できます。たとえば、Destination Port=50-80 を指定して、この範囲内のポートのすべてのトラフィックを対象とします。ハイフンを使用して、開始と終了の数字を区切ります。すべての数値フィールドに対して、範囲を使用できるわけではありません。たとえば、[Source] 要素に IP アドレスを範囲で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

イベントには次の情報を含めることができます。イベントの詳細を表示したときに、この情報を確認できます。最も興味のある情報を表示するためにイベント ビューア テーブルに列を追加することもできます。

使用可能なフィールドの完全なリストを以下に示します。すべてのフィールドがすべてのイベントタイプに適用されるわけではありません。個別のイベントで入手可能な情報は、システムで接続が記録された方法、理由、時期によって異なる可能性があることに注意してください。

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制御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

明示的に許可された接続。

信頼

信頼された接続。信頼ルールによって検出された TCP 接続の最初のパケットだけが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）]

ブロックされた接続。[ブロック（Block）]動作は、次の条件下で、アクセス許可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ブロックされた接続。
- 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。
- 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。
- SSL ポリシーによってブロックされた接続。

デフォルトアクション

接続がデフォルト アクションによって処理されました。

ファイルイベントまたはマルウェアイベントの場合は、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たファイル ルール アクションと、すべての関連するファイル 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、関連するビジネスとの関連性があります。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、アプリケーション タグ（Application Categories、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基準。

アプリケーションのリスク（Application Risk）

接続中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。

ブロック タイプ（Block Type）

イベントでトラフィック フローが一致したアクセス制御ルールで指定されたブロックのタイプ：block または interactive block。

クライアント アプリケーション、クライアント バージョン（Client Application、Client Version）

接続で検出されたクライアントのクライアント アプリケーションとバージョン。

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：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ます。このフィールドには、それらのうちの最も低いもの（関連性が最も薄いもの）が表示されます。

クライアント カテゴリ、クライアント タグ（Client Category、Client 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。

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：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ます。このフィールドには、それらのうちの最も高いものが表示されます。

接続（Connection）

内部的に生成された、トラフィック フローの一意の ID。

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

イベントでトラフィック フローが一致したアクセス制御ルールで指定されたブロックのタイプ：block または interactive block。

接続のバイト数（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。

宛先国または大陸（Destination Country and Continent）

受信ホストの国と大陸。

宛先 IP

侵入、ファイル、またはマルウェア イベントで受信側ホストによって使用された IP アドレス。

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

セッション レスポンダによって使用されたポートまたは ICMP コード。

宛先セキュリティグループタグ、宛先セキュリティグループタグ名

宛先に関連付けられている TrustSec セキュリティグループタグの番号と名前（存在する場合）。

方向（Direction）

ファイルの伝送方向。

判定結果（Disposition）

ファイルの評価：

[マルウェア（Malware）]

Secure Malware Analytics Cloud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、またはファイルの脅威スコアが、ファイルポリシーで定義されたマルウェアしきい値を超えていることを示します。ローカルマルウェア分析では、ファイルをマルウェアとしてマークすることもできます。

[クリーン（Clean）]

Secure Malware Analytics Cloudでそのファイルがクリーンとして分類されているか、ユーザー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

システムが Secure Malware Analytics Cloudに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、Secure Malware Analytics Cloudがファイルを正しく分類していませんでした。

カスタム検出

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。

応対不可

システムが Secure Malware Analytics Cloudに問い合わせることができなかったことを示します。この評価を持つイベントのパーセンテージが低く表示される場合があります。これは、想定された動作です。

[該当なし（N/A）]

ファイル検出ルールまたはファイルブロックルールでファイルが処理され、システムが Secure Malware Analytics Cloudに問い合わせなかったことを示します。

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

接続がデバイスから出たインターフェイスとゾーン。

[出力仮想ルータ（Egress Virtual Router）]

宛先インターフェイスが属する仮想ルータ(存在する場合)の名前。

イベント、イベント タイプ（Event、Event Type）

イベントのタイプ。

イベント秒、イベント マイクロ秒（Event Seconds、Event Microseconds）

イベントが検出された、秒単位およびミリ秒単位の時間。

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 Documents、Archive、Multimedia、Executables、PDF files、Encoded、Graphics、System Files 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）

ファイルの名前です。

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、すべての関連するファイル ルール アクションのオプション。

[ファイルSHA-256（File SHA-256）]

ファイルの SHA-256 ハッシュ値。

ファイル サイズ（KB）（File Size (KB)）

キロバイト単位のファイルのサイズ。ファイル サイズは、システムが受信を完了する前にファイルをブロックした場合に空白になる可能性があります。

ファイル タイプ（File Type）

ファイルのタイプ（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たファイル 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）

イベントでトラフィック フローが一致したファイル ルールで指定されたブロックのタイプ：block または interactive block。

ファイアウォール ポリシー ルール。ファイアウォール ルール（Firewall Policy Rule、Firewall Rule）

接続を処理したアクセス制御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 Referrer

接続で検出されたHTTPトラフィックの要求されたURLの参照元を表すHTTP参照元（別のURLへのリンクを提供したWebサイトや別のURLからのリンクをインポートしたWebサイトなど）。

HTTP レスポンス（HTTP Response）

接続で、クライアントの HTTP 要求に応答して送信された HTTP ステータス コード。

IDS 分類（IDS Classification）

イベントを生成したルールが属している分類。

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

接続がデバイスに入ったインターフェイスとゾーン。

[入力仮想ルータ（Ingress Virtual Router）]

送信元インターフェイスが属する仮想ルータ(存在する場合)の名前。

イニシエータ バイト、イニシエータ パケット（Initiator Bytes、Initiator Packets）

セッション イニシエータから送信されたバイトまたはパケットの総数。

イニシエータの国と大陸（Initiator Country and Continent）

セッションを開始したホストの国と大陸。イニシエータ IP アドレスがルーティング可能な場合にのみ使用できます。

イニシエータ IP（Initiator IP）

接続またはセキュリティ インテリジェンス イベントでセッションを開始したホスト IP アドレス（および DNS 解決が有効になっている場合のホスト名）。

インライン結果（Inline Result）

システムがインライン モードで動作している場合に、侵入イベントをトリガーしたパケットをドロップしたまたはドロップするはずだったかどうか。空白は、トリガーされたルールが Drop and Generate Events に設定されていなかったことを示します。

侵入ポリシー（Intrusion Policy）

イベントを生成したルールが有効になっていた侵入ポリシー。

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

イベントでトラフィック フローが一致した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に関連付けられたマルチプロトコル 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）

イベントでトラフィック フローが一致したファイル ルールで指定されたブロックのタイプ：block または interactive block。

メッセージ（Message）

侵入イベントの場合は、イベントの説明テキスト。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追加情報。

NAT宛先IP

ネットワークアドレス変換（NAT）の対象となるパケットの場合は、変換後の宛先 IP アドレス。

NAT宛先ポート

ネットワークアドレス変換（NAT）の対象となるパケットの場合は、変換後の宛先ポート。

NAT送信元IP

ネットワークアドレス変換（NAT）の対象となるパケットの場合は、変換後の送信元 IP アドレス。

NAT送信元ポート

ネットワークアドレス変換（NAT）の対象となるパケットの場合は、変換後の送信元ポート。

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）

セッションを開始した元のクライアント ホストの国と大陸。元の IP アドレスがルーティング可能な場合にのみ使用できます。

元のクライアント IP（Original Client IP）

HTTP 接続を開始したクライアントの元の IP アドレス。このアドレスは、X-Forwarded-For（XFF）ヘッダー フィールド、True-Client-IP HTTP ヘッダー フィールド、またはそれらの等価物から抽出されます。

ポリシー、ポリシー リビジョン（Policy、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）ルールを含む、アクセス コントロール ポリシーとそのリビジョン。

優先度（Priority）

Cisco Talos Intelligence Group（Talos）：[高（high）]、[中（medium）]、または [低（low）] によって決まるイベントの優先度。

プロトコル（Protocol）

接続に使用されたトランスポート プロトコル。

理由（Reason）

次の表に説明する状況で、接続がロギングされた理由。これ以外の場合、このフィールドは空です。

理由	説明
[DNS ブロック（DNS Block）]	システムは検査を行わず、ドメイン名とセキュリティ インテリジェンス データに基づいて接続を拒否しました。DNS ブロックの理由は、DNS ルール アクションに応じて、Block、Domain not found、または Sinkhole のアクションとペア化されます。

理由	説明
DNS モニタ	システムが、ドメイン名と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が、接続を拒否するのではなくモニタするように設定されていました。
エレファントフロー	接続は、エレファントフローと見なすのに十分な大きさです。このフローは、システム全体のパフォーマンスに影響を与えるのに十分な大きさです。デフォルトでは、エレファントフローとは 1GB/10 秒を超えるフローです。**system support elephant-flow-detection** コマンドを使用して、デバイス CLI でエレファントフローを識別するためのバイトしきい値と時間しきい値を調整できます。
ファイル ブロック	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ていました。ファイル ブロックの理由は、必ず、Block のアクションとペア化されます。
ファイル カスタム検出	接続に、システムが送信を阻止するカスタム検出リストにあるファイルが含まれていました。
ファイル モニタ	システムが、接続に特定のタイプのファイルを検出しました。
ファイル再開許可	ファイル伝送が、元はファイルブロックルールまたはマルウェアファイルブロックルールによってブロックされました。ファイルを許可する新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に再開しました。
[ファイル復帰ブロック（File Resume Block）]	ファイル伝送が、元はファイル検出ルールまたはマルウェア 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ました。ファイルをブロックする新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に停止しました。
[侵入ブロック（Intrusion Block）]	システムが、接続で検出しエクスプロイト（侵入ポリシー違反）をブロックしたまたはブロックするはずでした。侵入ブロックの理由は、ブロックされたエクスプロイトの場合は Block のアクションと、ブロックされるはずだったエクスプロイトの場合は Allow のアクションとペア化されます。
侵入モニタ	システムが、接続でエクスプロイト（侵入ポリシー違反）を検出しましたがブロックしませんでした。これは、トリガーされた侵入ルールの状態が Generate Events に設定されている場合に発生します。
IP ブロック	システムが検査する前に、IP アドレスとセキュリティ インテリジェンス データに基づいて接続を拒否しました。IP ブロックの理由は、必ず、Block のアクションとペア化されます。

理由	説明
保留中のルールの照合（Pending Rule Match）	これは、どのルールがマッチしているかをシステムが判断できるようになる前に接続が終了した場合に発生します。これらの短期間の接続（DNS ルックアップなど）は、通常、ファイアウォールを介して許可されます。特に、アクセス制御ポリシーの初めの部分にアプリケーションベースのルールがある場合、システムは少数のパケットを検査して、ルールがマッチしているか判断します。
SSL ブロック（SSL Block）	システムが、暗号化された接続を SSL インスペクション設定に基づいてブロックしました。[SSL ブロック（SSL 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。
[URLブロック（URL Block）]	システムが検査する前に、URL とセキュリティ インテリジェンス データに基づいて接続を拒否しました。URL ブロックの理由は、必ず、Block のアクションとペア化されます。

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）

接続のプロトコルが HTTP または HTTPS の場合は、このフィールドにそれぞれのプロトコルで使用されていたホスト名が表示されます。

レスポンダ バイト、レスポンダ パケット（Responder Bytes、Responder Packets）

セッション レスポンダから送信されたバイトまたはパケットの総数。

レスポンダの国と大陸（Responder Country and Continent）

セッションに応答したホストの国と大陸。レスポンダ IP アドレスがルーティング可能な場合にのみ使用できます。

レスポンダ IP（Responder IP）

接続またはセキュリティ インテリジェンス イベントのセッションレスポンダのホスト IP アドレス（および DNS 解決が有効になっている場合のホスト名）。

SI カテゴリ ID（セキュリティ インテリジェンス カテゴリ）

ネットワーク名や URL オブジェクト名、フィードカテゴリの名前など、ブロック項目が含まれるオブジェクトの名前。

署名（Signature）

ファイル/マルウェア イベントの署名 ID。

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

送信ホストの国と大陸。送信元 IP アドレスがルーティング可能な場合にのみ使用できます。

送信元 IP（Source IP）

侵入、ファイル、マルウェア イベントで送信側ホストによって使用された IP アドレス。

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

セッション イニシエータによって使用されたポートまたは ICMP タイプ。

送信元セキュリティグループタグ、送信元セキュリティグループタグの名前

送信元に関連付けられているTrustSecセキュリティグループタグの番号と名前（存在する場合）。

実際のSSLアクション（SSL Actual Action）

システムによって接続に適用される実際のアクション。これは期待される動作とは異なることがあります。たとえば、接続が復号化を適用するルールと一致しても、いくつかの理由で復号化できないことがあります。

アクション	説明
ブロック/リセット付きブロック（Block/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）	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）	置換された公開キーによる自己署名サーバ証明書を使用して復号された発信接続を表します。
復号（既知のキー）	既知の秘密キーを使用して復号された着信接続を表します。
デフォルトアクション	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	システムが復号化しなかった接続を表します。

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

証明書の認証に使用する SHA ハッシュ値。

SSL 証明書ステータス（SSL Certificate Status）

これは、証明書ステータスSSLルールの条件を設定した場合にのみ適用されます。暗号化されたトラフィックがSSLルールと一致する場合、次のサーバ証明書のステータス値の1つ以上がこのフィールドに表示されます。

- 自己署名
- 有効

- 署名が無効です
- 発行者が無効です
- 期限切れ
- 不明
- まだ有効ではありません
- 破棄

復号できないトラフィックが SSL ルールと一致する場合、[チェックしていない（Not Checked）] がこのフィールドに表示されます。

SSLサイファスイート（SSL Cipher Suite）

接続に使用された暗号スイート。

予期されたSSLアクション（SSL Expected Action）

接続が一致した SSL ルールで指定されたアクション。

[SSLフローフラグ（SSL Flow Flags）]

暗号化された接続の最初の 10 デバッグ レベル フラグ。

SSL フローメッセージ（SSL Flow Messages）

HELLO_REQUEST や CLIENT_HELLO など、SSL ハンドシェイク中にクライアントとサーバ間で交換された SSL/TLS メッセージ。TLS 接続で交換されたメッセージの詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。

SSL ポリシー（SSL Policy）

接続に適用された SSL 復号ポリシーの名前。

SSL ルール（SSL Rule）

接続に適用された SSL 復号ルールの名前。

SSL セッション ID（SSL Session ID）

SSL ハンドシェイク中にクライアントとサーバ間でネゴシエートされた 16 進数のセッション ID。

SSL チケット ID（SSL Ticket ID）

SSL ハンドシェイク中に送信されたセッション チケット情報の 16 進数のハッシュ値。

SSL URL カテゴリ（SSL URL Category）

SSL 復号処理中に決定された宛先 Web サーバの URL カテゴリ。

SSL バージョン（SSL Version）

接続に使用された SSL/TLS バージョン。

TCP フラグ（TCP Flags）

接続で検出された TCP フラグ。

合計パケット数（Total Packets）

接続で送信されたパケットの総数：**イニシエータ パケット** + **レスポンダ パケット**。

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

セッション中にモニタ対象ホストによって要求された URL と、それに関連付けられたカテゴリ、レピュテーション、レピュテーション スコア（使用可能な場合）。

DNSルックアップ要求フィルタリングの場合、カテゴリとレピュテーションは[DNSクエリ]フィールドに表示されるFQDN用です。Web要求ではなくDNS要求に対してカテゴリ/レピュテーションルックアップが実行されるため、URLフィールドは空白になります。

システムが SSL アプリケーションを識別またはブロックした場合は、要求された URL が暗号化トラフィック内に存在するため、システムはSSL証明書に基づいてトラフィックを識別します。したがって、SSLアプリケーションの場合は、URLが証明書に含まれている共通名を示します。

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た一番内側の 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：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ます。このフィールドには、それらのうちの最も低いもの（関連性が最も薄いもの）が表示されます。

Web アプリケーション カテゴリ、Web アプリケーション タグ（Web App Categories、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、Web アプリケーションの特性を示す基準。

Web アプリケーション 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：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ます。このフィールドには、それらのうちの最も高いものが表示されます。

Web アプリケーション（Web Application）

接続で検出された HTTP トラフィックの内容または要求された URL を表す Web アプリケーション。

Web アプリケーションがイベントの URL と一致しなかった場合は、そのトラフィックがアドバタイズメント トラフィックなどの参照先のトラフィックの可能性があります。システムが参照先のトラフィックを検出すると、参照元のアプリケーション（使用可能な場合）を保存し、そのアプリケーションを Web アプリケーションとしてリストします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。