# 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モニター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にロギングを有効にする

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、幅広いトラフィック統計をモニターできます。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、イベントおよび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。

**Connection Events**

ユーザー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。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。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。

**Intrusion Events**

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、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**

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。マルウェア防御 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。マルウェア防御 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。

**Security Intelligence Events**

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ーされた各接続の、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（ユーザー 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上およびコンプライアンス上の要件に従って接続をロギングしてください。生成するイベントの数を抑え、パフォーマンスを向上させることが目標である場合は、分析のために重要な接続のロギングのみを有効にします。しかし、プロファイリングの目的でネットワーク トラフィックの広範な表示が必要な場合は、追加の接続のロギングを有効にできます。

システムは 1 つの接続をさまざまな理由でロギングすることがあるため、1 ヵ所でロギングを無効にしても、一致する接続がロギン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する各ルール（およびデフォルトのアクション）でこれ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のフィルタリングの結果、システムが接続イベントをロギングすると、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。その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。
- 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の場合、システムは即座にセッションを終了し、イベントを生成します。監視対象の接続やアクセス コントロール ルールに渡す接続の場合、システムはセッションが終了するとイベントを生成します。

# 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。
- システムは、ファイル イベントとマルウェア イベントに関連付けられた接続を自動的にログに記録します。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 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、トラフィックをさらに検査し、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。侵入またはファイル ポリシーが接続をブロックする理由を発見した場合、接続ログ設定を問わず、システムは接続終了イベントをただちにログに記録します。ロギングが許可された接続は、ネットワーク内のトラフィックのほとんどの統計情報を提供します。
- 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。ただし、信頼されている接続では、ディスカバリ データ、侵入、または禁止されたファイルやマルウェアがインスペクションされません。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するアクセス 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 アクションの場合は、システムは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、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）攻撃の間にブロックされた TCP 接続をロギングすると、システム パフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロック ルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニターするかどうかを検討します。
- 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 サーバー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 サーバーに送信するには、侵入ポリシーの設定でサーバーを設定します。Syslog サーバーにファイル/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）]** でサーバーを設定します。

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 サーバー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。

# トラフィックのモニタリングおよびシステム ダッシュボード

システムには、デバイスを通過するトラフィックおよびセキュリティ ポリシーの結果を分析するために使用できる複数のダッシュボードがあります。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。

ハイ アベイラビリティ 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。自分にとって重要な情報をログに記録するルールを設定してください。また、ユーザー情報はユーザー ID を収集するアイデンティティ ルールを設定している場合にのみ利用できます。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と表に表示されるデータを制御するために、定義済みの時間範囲（最後の時間や週など）を選択できます。また、特定の開始時刻と終了時刻を指定してカスタムの時間範囲を定義することもできます。

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含まれます。

- 上位 5 つの棒グラフ：これらのグラフは [ネットワークの概要（Network Overview）] ダッシュボードに表示されます。また、ダッシュボードテーブルで項目をクリックした場合、項目ごとのサマリーのダッシュボードにも表示されます。[トランザクション（Transactions）] または [データの使用状況（Data Usage）]（送受信バイトの合計）のカウント間で情報を切り替えることができます。すべてのトランザクション、許可トランザクション、または拒否トランザクションを表示するために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、そのリンクをクリックして、より詳細な情報が含まれているサマリー ダッシュボードを表示します。

**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。

- [ユーザー（Users）]：ネットワークの上位ユーザーが表示されます。ユーザー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。ユーザー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）]：ユーザーは認証を求められましたが、最大許容試行回数内に有効なユーザー名/パスワードのペアを入力できませんでした。認証の失敗は、それ自体ではユーザーのネットワークへのアクセスは妨げられませんが、これらのユーザーのネットワーク アクセスを制限するためのアクセス ルールを記述できます。

  - [ゲスト（Guest）]：ゲストユーザーは、これらのユーザーをゲストと呼ぶようにアイデンティティ ルールが設定されている点を除き、認証失敗ユーザーと同様です。ゲストユーザーは認証を求められましたが、最大試行回数内に認証されることができませんでした。

  - [認証不要（No Authentication Required）]：ユーザーの接続が認証なしに指定されたアイデンティティ ルールに一致したため、ユーザーは認証を求められませんでした。

- [不明（Unknown）]：IPアドレスのユーザーマッピングがなく、認証失敗の記録もありません。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い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。接続は、「許可」ルールと一致するか、またはゾーン、アドレス、およびポート以外の基準を使用するブロック ルールと一致するかどうかのインスペクションが実行されます。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 トラフィックの上位の宛先が表示されます。
- [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 ルールに侵入ポリシーを設定する必要があります。
- [ターゲット（Targets）]：攻撃の被害者である、侵入イベントの上位のターゲットが表示されます。この情報を表示するには、アクセス ルールに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 ルールに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 トラフィックで確認された上位のファイル 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。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を表示するように、スループット グラフを制限できます。

（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）]：イベント発生時にイベントが表示する場合に選択します。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、ユーザーの接続の問題を解決するのに役立ちます。
- [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の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（CLI（コマンドライン インターフェイス）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 サーバー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 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。

### 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。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 （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。
- 新しいイベントの表示速度を制御するには、別のリフレッシュ レート（5、10、20、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 （11 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 （13 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 （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。

# 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、イベントの表示に必要な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、ビュー 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 [追加/削除カラム（Add/Remove Columns）] アイコン ボタンをクリックし、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 （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。

### カラムのクリック

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、ドロップダウンから目的の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オペレータが含まれます。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、フィールドに入力してオペレータまたは値を調整できます。テーブルにフィルタを適用するには、[フィルタ（Filter）]をクリックします。

### 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。 |
| > | 次の値より大きい。イベントに、指定した値よりも大きい値が含まれます。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、送信元としてこれらのいずれかのアドレスを持つイベントが照合されます。
- 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持つイベントが照合されます。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取得できます。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、[送信元（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が含まれます。これらの情報は、イベントの詳細情報を表示すると確認できます。また、イベント ビューア表に列を追加すると、最も関心のある情報を表示できます。

以下に、使用可能なフィールドの完全なリストを示します。すべてのフィールドがどのイベントタイプにも適用されるわけではありません。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、どのようにして接続を記録したか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（Allow）]**

明示的に許可された接続。

**[信頼（Trust）]**

信頼できる接続。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）]**

ブロックされている接続。[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。
- ファイルがファイル ポリシーによってブロックされている接続。
- 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ている接続。

**[デフォルトアクション（Default Action）]**

接続はデフォルト 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。

**[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するビジネスとの関連性：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、クライアントタグ（Client Application, Client Version）]**

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。

**[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 アドレス（Destination 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 レスポンダが使用するポートまたは 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）]**

ファイルの送信方向。

**[傾向（Disposition）]**

ファイルの性質。

**[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。

**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。

**Unavailable**

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（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）]**

接続がデバイスを通り抜けたゾーンとインターフェイス。

**[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時刻（秒またはマイクロ秒単位）。

**[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）]**

ファイルの名前。

**[ファイルルールのアクション（File Rule Action）]**

ファイルを検出したファイル ポリシー ルールに関連したアクション、および関連するファイル アクション 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（File Size）（KB）]**

ファイルのサイズ（KB 単位）。システムがファイルを完全に受信する前にブロックした場合、ファイル サイズが空白になる場合があります。

**[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 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）]**

クライアントからの接続経由のHTTP要求に応じて送信される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ゾーンとインターフェイス。

**[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 イニシエータが送信した合計バイト数またはパケット数。

**[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の所在地の国と地域の名前。イニシエータの IP アドレスがルーティング可能であるとき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）]**

インラインモードで動作しているときに、侵入イベントをトリガーしたパケットをシステムがドロップした、またはドロップするはずだったか。ブランクは、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（Intrusion Policy）]**

イベントを生成したルールが有効に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、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ている追加情報。

**NAT 宛先 IP（NAT Destination 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（NAT Destination Port）**

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（NAT Source 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（NAT Source Port）**

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所在地の国と地域の名前。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ときにのみ使用できます。

**[クライアントのオリジナル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）または True-Client-IP HTTP のヘッダー フィールド、またはそれらの同等品から取得されます。

**[ポリシー、ポリシーの改訂（Policy, Policy Revision）]**

アクセス コントロール ポリシーとその改訂版。イベントに関連付けられているアクセス（ファイアウォール）ルールを含みます。

**[プライオリティ（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）]**

接続に使用されるトランスポート プロトコルです。

**[理由（Reason）]**

次の表では、接続が記録された理由を説明しています。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）] | 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、インスペクションなしで接続が拒否されました。[DNS ブロック（DNS Block）] の理由は、DNS ルール アクションに応じて、[ブロック（Block）]、[ドメインが見つかりません（Domain not found）]、[シンクホール（Sinkhole）] のアクションと対として組み合わされます。 |
| DNS モニタ（DNS Monitor） | システムは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でしたが、システムは接続を拒否するのではなくモニターするように設定されています。 |
| 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（File Block）] | 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でいます。[ファイルブロック（File Block）] の理由は必ず [ブロック（Block）] 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） | 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でいます。 |
| [ファイルモニタ（File Monitor）] | 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ました。 |
| [ファイル復帰許可（File Resume Allow）] | ファイル送信がはじめに [ファイルブロック（Block Files）] ルールまたは [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）] | ファイル送信がはじめに [ファイル検出（Detect Files）] ルールまたは [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。 |

| 理由 | 説明 |
|---|---|
| [侵入ブロック（Intrusion Block）] | 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、ブロックするはずでした。[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。 |
| [侵入モニター（Intrusion Monitor）] | 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。 |
| [IPブロック（IP Block）] | 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、インスペクションなしで接続が拒否されました。[IPブロック（IP 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。 |
| [SSL ブロック（SSL Block）] | システムが SSL インスペクション設定に基づいて暗号化接続をブロックしました。[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）] | URL とセキュリティ 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が拒否されました。[URLブロック（URL 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。 |

**[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 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、レスポンダパケット（Responder Bytes, Responder Packets）]**

セッション レスポンダが送信した合計バイト数またはパケット数。

**[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の所在地の国と地域の名前。レスポンダの IP アドレスがルーティング可能であるとき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)（SI Category ID (Security Intelligence Category)）]**

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。

**[シグネチャ（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であるときにのみ使用できます。

**[ソース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 イニシエータが使用するポートまたは 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 タグ名**

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）（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。 |

| アクション | 説明 |
|---|---|
| [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。 |

**[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、認証ステータスのSSLルール条件が設定されている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ルールに一致すると、このフィールドに次のサーバの証明書のステータス値の 1 つ以上が表示されます。

- [自署（Self Signed）]
- [有効（Valid）]
- [署名が無効（Invalid Signature）]
- [発行元が無効（Invalid issuer）]
- [期限切れ（Expired）]
- [不明（Unknown）]
- [まだ有効ではない（Not Valid Yet）]
- [失効（Revoked）]

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暗号スイート（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 ハンドシェイク時にクライアントとサーバー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。

**[SSLURL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）]**

セッション中に監視対象のホストによって要求されたURLと、関連付けられたカテゴリ、レピュテーション、およびレピュテーション スコア（利用できる場合）。

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（DNS Query）] 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する場合、要求された URL は暗号化トラフィック内にあるため、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、この URL は証明書に含まれる一般名を表示します。

**[ユーザー（User）]**

イニシエータの IP アドレスに関連付けられたユーザー。

**[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およびタグ（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（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 に一致しない場合、そのトラフィックは通常、参照先のトラフィックです（アドバタイズメントのトラフィックなど）。システムは、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を保存し（可能な場合）、そのアプリケーションを Web アプリケーションとして表示します。

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。