接続およびセキュリティ インテリジェンスのデータの使用

FireSIGHT システムの管理対象デバイスは、ネットワーク上のホストで生成されたトラフィックを継続的に監視します。ネットワーク トラフィックが特定の条件に一致する場合に*接続イベント*を生成するアクセス コントロール機能を使用できます。接続イベントには、検出されたセッションに関する、タイムスタンプ、IP アドレス、位置、アプリケーションなどのデータが含まれます。

トラフィックをブラックリストに記載するか、セキュリティ インテリジェンス データに基づいてブラックリストに記載されたトラフィックを監視するようシステムが設定されている場合（Protection ライセンスが必須）、*セキュリティ インテリジェンス イベント*を表示できます。これは、ブラックリストまたは監視の決定を表す特殊な種類の接続イベントです。セキュリティ インテリジェンス イベントは似ていても別々に保存およびプルーニングされ、それぞれのイベント ビュー、ワークフロー、カスタム分析のダッシュボード ウィジェットのプリセットを持ちます。セキュリティ インテリジェンス イベントは接続イベントのサブセットであるため、接続イベントに関する一般情報がセキュリティ インテリジェンス イベントにも付属します（特に注記がない限り）。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 リストとフィードの操作」（P.5-4）および「セキュリティ インテリジェンス データに基づくトラフィックのフィルタリング」（P.13-13）を参照してください。

防御センター データベースに接続イベントをロギングすると、FireSIGHT システムの分析、レポート作成、相関機能を活用することができます。また、syslog または SNMP トラップ サーバにほとんどの接続イベントを送信できます。

管理対象デバイスで収集された接続データを補うために、NetFlow 対応デバイスによって生成されたレコードを使用して接続イベントを生成できます。シスコの管理対象デバイスによって監視できない NetFlow 対応デバイスがネットワークに配置されている場合は特に有効です。

多くの接続イベントで提供される地理情報をさらに強化するために、地理情報の更新をシステムに設定することもできます。地理情報の詳細については、「地理情報の使用」（P.47-24）を参照してください。

詳細については、以下を参照してください。

接続データについて

ライセンス：任意

管理対象デバイスが監視するネットワークに対して、次の場合に接続イベントをロギングするアクセス コントロール ポリシーを設定して適用できます。

- ネットワーク トラフィックがブラックリストに記載されるか、監視対象となった場合。これは、セキュリティ インテリジェンス イベントも作成します。
- ネットワーク トラフィックが、監視以外のアクセス コントロール ルールの条件を満たした場合。
- ネットワーク トラフィックがアクセス 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た場合。
- ネットワーク トラフィックが、1 つ以上の Monitor ルールの条件を満たした場合（自動的に有効化）。
- アクセス コントロール ルールに関連付けられた侵入ポリシーがイベントを生成した場合（自動的に有効化）。
- アクセス コントロール ルールに関連付けられたファイル ポリシーがファイルを検出またはブロックしたか、マルウェアを検出またはブロックした場合（自動的に有効化）。

接続ログを個々のアクセス コントロール ルール、ポリシー、設定に結び付けることで、ロギング対象の接続をきめ細かく制御できます。

NetFlow のデータ収集はアクセス コントロール ルールにリンクされていないため、ロギングする NetFlow 接続については、きめ細かい制御ができないことに注意してください。シスコの管理対象デバイスは NetFlow 対応デバイスによってエクスポートされるレコードを検出し、それらのレコードのデータに基づいて単一方向の接続終了イベントを生成し、最終的にそのイベントをデータベースに記録するために防御センターへ送信します。システム ログまたは SNMP トラップ サーバに NetFlow イベントは送信できません。NetFlow でロギングされた接続は [Security Intelligence Category] フィールドの値を持つことができないため、セキュリティ インテリジェンス イベントとしては表示されません。

接続のロギングの詳細については、次の項を参照してください。

- 「接続、ファイル、マルウェアに関する情報のロギング」（P.14-39）では、アクセス コントロール ルールの条件を満たすトラフィックをロギングする方法について説明しており、それらの接続をロギングするタイミングと方法についての一般的なガイダンスも含まれています。この項では、接続のロギングがルールのアクションによってどのように影響を受けるか、また接続データのロギングが侵入、ファイル、マルウェアのイベント ロギングにどのように関連しているかについても説明しています。
- 「ブラックリスト登録された接続のロギング」（P.13-20）では、セキュリティ インテリジェンス機能を使用して、接続を拒否するか（ブラックリストに記載）、インスペクションを行う（ブラックリストを監視のみに設定）方法について説明しています。
- 「デフォルト アクションの接続のロギング」（P.13-8）では、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た接続をロギングする方法について説明しています。
- 「NetFlow について」（P.35-19）では、NetFlow に関するより詳細な情報を提供するとともに、NetFlow 接続イベントを FireSIGHT システムによって監視されたトラフィックに基づく接続イベントと比較します。
- 「ネットワーク検出ポリシーの作成」（P.35-26）では、検出ポリシーを作成および管理する方法について説明しています。これは NetFlow データ収集の設定を行う場所でもあります。

次の表では、接続データをロギングするために必須のライセンスについて説明します。

表 16-1　接続データをロギングするためのライセンス要件

目的	必要なライセンス
NetFlow 接続のロギングなどの基本的な接続のロギングを行う	任意
接続ログの情報に基づいてネットワーク マップにホストやユーザ データなどのデータを追加する、または接続イベントに関連付けられた地理情報および IOC（侵害の痕跡）情報を参照する	FireSIGHT
次の接続をロギングする • セキュリティ インテリジェンスのフィルタリングの決定を表すもの（すべてのセキュリティ インテリジェンス イベントが含まれます） • 侵入の検出と防御を行うアクセス コントロール ルールの対象 • ファイルの管理を行うアクセス コントロール ルールの対象だが、高度なマルウェア対策の対象ではない場合	Protection
高度なマルウェア対策を行うアクセス コントロール ルールの対象となる接続をロギングする	Malware
アプリケーションまたはユーザの制御を行うアクセス コントロール ルールの対象となる接続をロギングする	Control
URL カテゴリとレピュテーション データを使用する URL 条件を持つアクセス コントロール ルールの対象となる接続をロギングする 監視対象ホストが要求した URL の URL カテゴリおよび URL レピュテーション情報を表示する	URL Filtering

ここでは、検出された接続に関する入手可能な情報の種類の詳細と、分析の一部として接続データをロギングし、集約し、使用する方法について説明します。

- 「接続サマリーについて」（P.16-3）
- 「接続およびセキュリティ インテリジェンスのデータ フィールド」（P.16-5）
- 「接続およびセキュリティ インテリジェンスのイベントで利用可能な情報」（P.16-11）
- 「FireSIGHT システムでの接続データの使用」（P.16-14）

接続サマリーについて

ライセンス：任意

FireSIGHT システムは 5 分間隔で収集された接続データを接続サマリーに集約します。システムはこれを使用して接続グラフとトラフィック プロファイルを生成します。必要に応じて、接続サマリーのデータに基づいてカスタム ワークフローを作成できます。これは、個々の接続イベントに基づいたワークフローと同じように使用できます。

セキュリティ インテリジェンス イベント専用の接続 サマリーはないことに注意してください。ただし、対応する接続終了イベントは接続サマリーのデータに集約できます。

集約するには、複数の接続が次のとおりでなければなりません。

- 接続終了を表している
- 送信元と宛先の IP アドレスが同じで、応答側（宛先）のホストで同じポートを使用している
- 同じプロトコルを使用している（TCP または UDP）
- 同じアプリケーション プロトコルを使用している
- 同じシスコ管理対象デバイスで検出されているか、同じ NetFlow 対応デバイスによってエクスポートされている

各接続サマリーには、総合的なトラフィック統計情報のほか、サマリーの接続数も含まれています。NetFlow 対応デバイスは単一方向接続を生成するので、NetFlow データに基づいて接続ごとにサマリーの接続数が 2 ずつ増えます。

接続サマリーには、サマリーに集約された接続に関連付けられたすべての情報が含まれているのではないことに注意してください。たとえば、接続サマリーに接続を集約する際にクライアント情報は使用されないため、サマリーにクライアント情報は含まれません。

詳細については、次の項を参照してください。

- 「長時間接続」（P.16-4）
- 「外部応答側からの結合された接続サマリー」（P.16-4）
- 「接続およびセキュリティ インテリジェンスのイベントで利用可能な情報」（P.16-11）

長時間接続

ライセンス：任意

接続データを集約する 5 分間隔の 2 回以上に監視対象のセッションがまたがる場合、その接続は*長時間接続*と見なされます。接続サマリーで接続数を計算する際には、長時間接続が開始された 5 分間隔の回のみカウントします。

また、長時間接続において発信側と応答側が送信したパケット数とバイト数を計算する際は、システムは 5 分間隔の各回で実際に送信されたパケット数とバイト数を報告しません。代わりにシステムは、送信された合計パケット数と合計バイト数、接続の長さ、5 分間隔の各回で接続のどの部分が行われたかに基づいて、一定の送信速度を仮定し、値を推定します。

外部応答側からの結合された接続サマリー

ライセンス：任意

接続データの保存に必要なスペースを減らし、接続グラフのレンダリングを高速化するために、システムは次の場合に接続サマリーを結合します。

- 接続に関連するホストの 1 つが監視対象のネットワーク上にない場合
- 外部ホストの IP アドレスを除き、サマリーに含まれる接続が「接続サマリーについて」（P.16-3）に記載された集約の要件を満たしている場合（プロトコル、アプリケーション プロトコル、検出デバイスなど）

イベント ビューアで接続サマリーを表示する場合や、接続グラフを使用する場合、システムは非監視対象ホストの IP アドレスの代わりに `external` と表示します。

この集約の結果として、外部応答側を含む接続サマリーまたはグラフから接続データのテーブル ビューにドリルダウンしようとすると（つまり、個別の接続データへのアクセス）、テーブル ビューには情報が何も表示されません。

接続およびセキュリティ インテリジェンスのデータ フィールド

ライセンス：機能に応じて異なる

サポート対象デバイス：シリーズ 3、VirtualX-Series、ASA FirePOWER

サポート対象防御センター：任意（DC500 を除く）

各接続のテーブル ビューまたは接続グラフには、表示している接続または接続サマリーのタイムスタンプ、IP アドレス、地理情報、アプリケーションなどの情報が含まれています。セキュリティ インテリジェンス イベントのビューには接続イベントのビューと同じ一般情報が含まれていますが、[Security Intelligence Category] の値が割り当てられている接続のみ表示します。NetFlow でロギングされた接続データは [Security Intelligence Category] の値を持つことができないため、セキュリティ インテリジェンス イベントの NetFlow データのフィールドに値が入力されることはありません。セキュリティ インテリジェンス イベントを表示するには、アプライアンスに Protection ライセンスが必須です。DC500 防御センターおよび シリーズ 2 の管理対象デバイスはどちらもセキュリティ インテリジェンス機能をサポートしていないことに注意してください。

次のリストでは、FireSIGHT システムによってロギングされた接続データを詳しく説明します。個々の接続またはセキュリティ インテリジェンス イベントでロギングされる情報を決定する要素についての説明は、「接続およびセキュリティ インテリジェンスのイベントで利用可能な情報」（P.16-11）のセクションを参照してください。一部のデータ フィールドは、特定のライセンス要件を満たす場合に限り使用できることに注意してください。詳細については、「接続データをロギングするためのライセンス要件」の表を参照してください。

Access Control Policy

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 アクションを含むアクセス コントロール ポリシー。

Access Control 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。

接続が 1 つの Monitor ルールに一致した場合、防御センターは接続を処理したルールの名前を表示し、その後に Monitor ルール名を表示します。接続が複数の Monitor ルールに一致したときは、イベント ビューアは一致した Monitor ルールの数を `Default Action + 2 Monitor Rules` などと表示します。

接続に一致した最初の 8 つの Monitor ルールのリストをポップアップ ウィンドウに表示するには、[*N* Monitor Rules] をクリックします。

Action

次の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。

- [Allow] は、明示的に許可され、インタラクティブにユーザがバイパスした、ブロックされた接続を表します。
- [Trust] は、信頼できる接続を表します。システムは、信頼ルールによって検出された TCP 接続をアプライアンスに応じて別にロギングすることに注意してください。

  シリーズ 2、仮想アプライアンス、Sourcefire Software for X-Seriesでは、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、最終セッションのパケットの 1 時間後にイベントを生成します。

シリーズ 3 アプライアンスでは、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、監視ルールの有無に応じて異なるイベントを生成します。監視ルールがアクティブな場合、システムはパケットを評価し、開始および接続終了イベントの両方を生成します。アクティブな監視ルールがない場合、システムは接続終了イベントだけを生成します。

- [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、[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。
- [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、Monitor 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、Monitor 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。

Application Protocol

接続で検出された、ホスト間の通信を表すアプリケーション プロトコル。

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、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。詳細については、「アプリケーションの特徴」の表を参照してください。

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、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。詳細については、「アプリケーションの特徴」の表を参照してください。

Category, Tag (Application Protocol, Client, Web Application)

アプリケーションの機能を理解するのに役立つ、アプリケーションを特徴付ける条件。詳細については、「アプリケーションの特徴」の表を参照してください。

Client and 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。

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。

Connections

接続サマリーに含まれる接続数。長時間接続（複数回の接続サマリー間隔にまたがる接続）の場合、最初の接続サマリー間隔の分だけ増加します。

Count

各行に表示される情報に一致する接続数。同一の行が複数作成される制約を適用した後にのみ、[Count] フィールドが表示されることに注意してください。

注　カスタム ワークフローを作成し、ドリルダウン ページに [Count] カラムを追加しない場合、各接続は個別に表示され、パケット数とバイト数は合計されません。

Device

接続を検出した管理対象デバイス。または、NetFlow 対応デバイスからエクスポートされた接続の場合は、NetFlow データを処理した管理対象デバイス。

Files

接続に関連付けられたファイル イベント（ある場合）。ファイル リストの代わりに、防御センターはファイル表示アイコン（  ）をこのフィールドに表示します。アイコンの数字は、その接続で検出またはブロックされたファイル数（マルウェア ファイルを含む）を示します。

アイコンをクリックするとポップアップ ウィンドウが表示され、接続で検出されたファイルのリストとともに、そのタイプと、該当する場合はマルウェアのルックアップ処理が示されます。

DC500 防御センターおよび シリーズ 2 デバイスはどちらもネットワークベースのマルウェア ファイル検出をサポートしていないことに注意してください。

詳細については、「接続で検出されたファイルの表示」（P.16-29）を参照してください。

First Packet or Last Packet

セッションの最初または最後のパケットが検出された日時。

Ingress Interface or Egress Interface

接続に関連付けられた入力または出力のインターフェイス。

Ingress Security Zone or Egress Security Zone

接続に関連付けられた入力または出力のセキュリティ ゾーン。

Initiator Bytes or Responder Bytes

セッションの開始側またはセッションの応答側が送信した合計バイト数。

Initiator Country or Responder Country

ルーティング可能な IP が検出された場合に、セッションを開始したホスト IP アドレスまたはセッションの応答側に関連付けられた国。その国の国旗のアイコンとともに、その国の ISO 3166-1 alpha- 3 の国番号が表示されます。国旗アイコンの上にポインタを移動すると、国の完全な名称が表示されます。

DC500 防御センターはこの機能をサポートしていないことに注意してください。

Initiator IP or Responder IP

セッションを開始したか、またはセッション応答側として応答したホスト IP アドレス（DNS 解決が有効化されている場合はホスト名も）。ブラックリストに記載された接続でブラックリストに記載された IP アドレスを識別できるように、ブラックリストに記載された IP アドレスの横のアイコンは見た目が少し異なります。

Initiator Packets or Responder Packets

セッションの開始側またはセッションの応答側が送信した合計パケット数。

Initiator User

セッションの開始側にログインしていたユーザ。

Intrusion Events

接続に関連付けられた侵入イベント（ある場合）。イベント リストの代わりに、防御センターは侵入イベント表示アイコン（防御センター）をこのフィールドに表示します。防御センター

アイコンをクリックするとポップアップ ウィンドウが表示され、接続に関連付けられた侵入イベントのリストとともに、優先度と影響度が示されます。詳細については、「接続に関連付けられた侵入イベントの表示」（P.16-30）を参照してください。

IOC

接続にかかわったホストに対する侵害の痕跡（IOC）をこのイベントがトリガーとして使用するかどうか。IOC の詳細については、「侵害の兆候について」（P.35-23）を参照してください。

NetBIOS Domain

セッションで使用された NetBIOS ドメイン。

NetFlow Destination/Source Autonomous System

NetFlow 対応デバイスによってエクスポートされた接続の場合、接続のトラフィックの送信元または宛先に対する、Border Gateway Protocol の自律システム番号。

NetFlow Destination/Source Prefix

NetFlow 対応デバイスによってエクスポートされた接続の場合、送信元または宛先の IP アドレスに、送信元と宛先のプレフィクス マスクが追加されたもの。

NetFlow Destination/Source TOS

NetFlow 対応デバイスによってエクスポートされた接続の場合、接続トラフィックが NetFlow 対応デバイスに入ったか、NetFlow 対応デバイスから出たときの Type of Service（TOS）バイトの設定。

NetFlow SNMP Input/Output

NetFlow 対応デバイスによってエクスポートされた接続の場合、接続トラフィックが NetFlow 対応デバイスに入ったか、NetFlow 対応デバイスから出た際のインターフェイスのインターフェイス インデックス。

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] の理由は必ず [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。
- [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。
- [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。[Intrusion Block] の原因は、ブロックされたエクスプロイトの場合は [Block]、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になります。
- [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。

Security Context

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。システムは、マルチコンテキスト モードの ASA FirePOWER デバイスの場合のみ、このフィールドに値を入力することに注意してください。

Security Intelligence 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とフィード、いずれかのシスコ インテリジェンス フィードのカテゴリのうち、いずれかの名前です。[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。詳細については、「セキュリティ インテリジェンス データに基づくトラフィックのフィルタリング」（P.13-13）を参照してください。

また、DC500 防御センターおよび シリーズ 2 デバイスはどちらもこの機能をサポートしていないことに注意してください。

Source Device

接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス。管理対象デバイスによって接続が検出された場合、このフィールドには `FireSIGHT` の値が入ります。

Source Port/ICMP Type or Destination Port/ICMP Code

セッションの開始側またはセッションの応答側で使用されるポート、ICMP タイプ、または ICMP コード。

TCP Flags

接続で検出された TCP フラグ。

Time

システムが接続を接続サマリーに集約するために使用した 5 分間隔の終了時刻。

URL, URL Category, and 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と、関連付けられたカテゴリおよびレピュテーション（利用できる場合）。

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、このフィールドは証明書に含まれる一般名を表示します。詳細については、「アクセス コントロール ポリシーの詳細設定」（P.13-21）および「クラウド通信の有効化」（P.51-27）を参照してください。

DC500 防御センターおよび シリーズ 2 デバイスはどちらも、URL カテゴリとレピュテーション データをサポートしていないことに注意してください。

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。

HTTP トラフィックに含まれる特定の Web アプリケーションをシステムが特定できなかった場合、このフィールドには [Web Browsing] と表示されます。

接続およびセキュリティ インテリジェンスのイベントで利用可能な情報

ライセンス：機能に応じて異なる

サポート対象デバイス：シリーズ 3、VirtualX-Series、ASA FirePOWER

サポート対象防御センター：任意（DC500 を除く）

個別の接続、接続サマリー、セキュリティ インテリジェンス イベントについての利用可能な情報は、複数の要因によって異なります。セキュリティ インテリジェンス イベントには Protection ライセンスが必要です。DC500 防御センターおよび シリーズ 2 の管理対象デバイスはどちらもセキュリティ インテリジェンス機能をサポートしていないことに注意してください。

検出方法

TCP フラグ、NetFlow 自律システム、プレフィクス、および TOS データを除いて、NetFlow レコードで利用可能な情報は、管理対象デバイスを使用したネットワーク トラフィックの監視によって生成される情報よりも限定的です。詳細については、「FireSIGHT システムのアプリケーション プロトコルの識別」の表を参照してください。

ロギング方法

管理対象デバイスによって直接検出された接続の場合、アクセス コントロール ルールのアクション、デフォルト アクション、またはセキュリティ インテリジェンスのブラックリストに応じて、接続の開始か終了または両方の接続イベントをロギングできます。NetFlow ベースの接続は、接続終了と見なされます。

接続開始イベントは、セッション期間にわたってトラフィックを調査して判別する必要がある情報を持っていません（送信されたデータの合計量や、接続の最終パケットのタイムスタンプなど）。また、接続開始イベントがセッションのアプリケーションや URL トラフィックに関する情報を持っている保証はありません。

関連付けられたファイルおよび侵入ポリシー

ファイル ポリシーに関連付けられたアクセス コントロール ルールによってロギングされた接続にのみ、ファイル情報が含まれます。同様に、接続ログで侵入情報を参照するには、侵入ポリシーをアクセス コントロール ルールもしくはデフォルト アクションと関連付ける必要があります。

接続イベント タイプ

接続サマリーには、集約された接続に関連付けられたすべての情報が含まれているのではありません。たとえば、接続サマリーに接続を集約する際にクライアント情報は使用されないため、サマリーにクライアント情報は含まれません。

接続グラフは、接続終了ログのみを使用する接続サマリーのデータに基づいていることに注意してください。接続開始データだけをロギングした場合、接続グラフと接続サマリーのイベント ビューにはデータが含まれていません。

トラフィック タイプ

システムは、トラフィック内に存在する情報だけを報告します。たとえば、非 HTTP トラフィックは、URL または Web アプリケーションの情報を含んでいません。また、発信側ホストに関連付けられているユーザが存在することはありません。

その他の設定

アクセス コントロール ポリシーの詳細設定では、HTTP セッションの監視対象ホストによって要求された URL ごとにシステムが接続ログに保存する文字数を制御できます。この設定を使用して URL のロギングを無効化する場合、システムは接続ログで個々の URL を表示しませんが、カテゴリとレピュテーション データは参照できます（存在する場合）。

また、すべての接続イベントに [Reason] があるわけではありません。これは、Interactive Block の設定をユーザがバイパスした場合など、特定の状況でのみ値が入力されるフィールドです。「Reason」（P.16-9）を参照してください。

アプライアンス モデル

シリーズ 2 デバイスと DC500 防御センターは機能のサブセットのみをサポートしているため、次の接続データは DC500 で表示されず、シリーズ 2 で検出および提供されません。

- セキュリティ インテリジェンス データ（すべてのセキュリティ インテリジェンス イベントを含む）
- URL カテゴリとレピュテーション データ
- ネットワークベースのマルウェアの検出に関連付けられているファイル データ

また、DC500 防御センターは地理情報データをサポートしていないため、イベントの発信側または応答側の国を表示しません。

シリーズ 2 アプライアンス機能の概要については、「シリーズ 2 アプライアンス」（P.1-3）を参照してください。

次の表は、接続イベントおよびセキュリティ インテリジェンス イベントの各フィールドとともに、検出方法、ロギング方法、接続イベント タイプによってシステムがそのフィールドに情報を表示するかどうかを示します。セキュリティ インテリジェンス イベントは集約されないため、[Summary] カラムは接続イベントのサマリーについてのみ示されることに注意してください。

ヒント　接続イベントおよびセキュリティ インテリジェンス イベント両方のテーブル ビューでは、各アプリケーション タイプの [Source Device] フィールドと、[Category] および [Tag] フィールドは、デフォルトでは非表示です。イベント ビューに非表示フィールドを表示するには、検索条件を拡大し、[Disabled Columns] の下のフィールド名をクリックします。

表 16-2　ロギングおよび検出方法に基づいた接続およびセキュリティ インテリジェンスのデータ

	検出方法:		ロギング方法:		接続イベント:	
フィールド	FireSIGHT	NetFlow	開始	終了	個別	サマリー
Time	はい	はい	いいえ	はい	いいえ	はい
First Packet	はい	はい	はい	はい	はい	いいえ
Last Packet	はい	はい	いいえ	はい	はい	いいえ
Action	はい	いいえ	はい	はい	はい	いいえ
Reason	はい	いいえ	はい	はい	はい	いいえ
Initiator IP	はい	はい	はい	はい	はい	はい
Initiator Country	はい	いいえ	はい	はい	はい	はい
Initiator User	はい	はい	はい	はい	はい	はい
Responder IP	はい	はい	はい	はい	はい	はい

表 16-2　ロギングおよび検出方法に基づいた接続およびセキュリティ インテリジェンスのデータ （続き）

	検出方法:		ロギング方法:		接続イベント:	
フィールド	FireSIGHT	NetFlow	開始	終了	個別	サマリー
Responder Country	はい	いいえ	はい	はい	はい	はい
Security Intelligence Category	はい	いいえ	はい	いいえ	はい	いいえ
Ingress Security Zone	はい	いいえ	はい	はい	はい	はい
Egress Security Zone	はい	いいえ	はい	はい	はい	はい
Source Port/ICMP Code	はい	はい	はい	はい	はい	いいえ
Destination Port/ICMP Type	はい	はい	はい	はい	はい	はい
Application Protocol	はい	はい	利用可能な場合	はい	はい	はい
Client	はい	いいえ	利用可能な場合	はい	はい	いいえ
Client Version	はい	いいえ	利用可能な場合	はい	はい	いいえ
Web Application	はい	いいえ	利用可能な場合	はい	はい	いいえ
Category, Tag (Application Protocol, Client, Web Application)	はい	いいえ	利用可能な場合	はい	はい	いいえ
Application Risk	はい	いいえ	利用可能な場合	はい	はい	いいえ
Business Relevance	はい	いいえ	利用可能な場合	はい	はい	いいえ
URL	はい	いいえ	利用可能な場合	はい	はい	いいえ
URL Category	はい	いいえ	利用可能な場合	はい	はい	いいえ
URL Reputation	はい	いいえ	利用可能な場合	はい	はい	いいえ
IOC	はい	いいえ	はい	はい	はい	いいえ
Intrusion Events	はい	いいえ	いいえ	はい	はい	いいえ
Files	はい	いいえ	いいえ	はい	はい	いいえ
Access Control Policy	はい	いいえ	はい	はい	はい	いいえ
Access Control Rule	はい	いいえ	はい	はい	はい	いいえ
Device	はい	はい	はい	はい	はい	はい
Ingress Interface	はい	いいえ	はい	はい	はい	はい
Egress Interface	はい	いいえ	はい	はい	はい	はい
Security Context（ASA のみ）	はい	いいえ	はい	はい	はい	はい
TCP Flags	いいえ	はい	いいえ	はい	はい	いいえ
NetFlow Destination/Source Autonomous System	いいえ	はい	いいえ	はい	はい	いいえ
NetFlow Destination/Source Prefix	いいえ	はい	いいえ	はい	はい	いいえ
NetFlow Destination/Source TOS	いいえ	はい	いいえ	はい	はい	いいえ
NetFlow SNMP Input/Output	いいえ	はい	いいえ	はい	はい	いいえ
Source Device	はい	はい	FireSIGHT	はい	はい	はい
NetBIOS Domain	はい	いいえ	はい	はい	はい	いいえ

表 16-2　ロギングおよび検出方法に基づいた接続およびセキュリティ インテリジェンスのデータ （続き）

	検出方法:		ロギング方法:		接続イベント:	
フィールド	FireSIGHT	NetFlow	開始	終了	個別	サマリー
Initiator Packets	はい	はい	有用でない	はい	はい	はい
Responder Packets	はい	はい	有用でない	はい	はい	はい
Initiator Bytes	はい	はい	有用でない	はい	はい	はい
Responder Bytes	はい	はい	有用でない	はい	はい	はい
Connections	はい	はい	いいえ	はい	いいえ	はい
Count	はい	はい	はい	はい	はい	いいえ

FireSIGHT システムでの接続データの使用

ライセンス：任意

防御センター データベースに接続データをロギングすると、次のような FireSIGHT システムの多くの機能を活用することができます。

- [Connection Summary] ダッシュボードの表示。システムによってロギングされた接続の概要ビューが提供されます。「ダッシュボードの使用」（P.3-1）を参照してください。
- システムによってロギングされた接続の詳細情報の表示。グラフ形式や表形式での表示が可能です。「接続およびセキュリティ インテリジェンスのデータの表示」（P.16-14）を参照してください
- システムによってロギングされた接続に基づくレポートの作成。「レポートの操作」（P.44-1）参照してください。
- 接続データを使用した、トラフィック プロファイルと呼ばれる通常のネットワーク トラフィックのプロファイルの作成および表示。「トラフィック プロファイルの作成」（P.40-1）を参照してください
- システムが特定の接続データを検出したとき、またはトラフィック プロファイルが変更されたときに、相関イベントをトリガーして生成する相関ルールの作成。「相関ポリシーのルールの作成」（P.39-3）参照してください
- 相関ルールへの接続トラッカーの追加。ルールの最初の条件が満たされた後で、システムが特定の接続を追跡し、追加の条件を追跡対象の接続が満たした場合にのみ相関イベントを生成できるようにします。「経時的な接続データを使用した相関ルールの制約」（P.39-23）を参照してください

接続およびセキュリティ インテリジェンスのデータの表示

ライセンス：機能に応じて異なる

サポート対象デバイス：シリーズ 3、VirtualX-Series、ASA FirePOWER

サポート対象防御センター：任意（DC500 を除く）

接続データの詳細な情報を取得するために、システムは接続データをグラフおよび表形式で表示できます。接続データにアクセスしたときに表示されるページは、使用するワークフローによって異なります。定義済みのワークフローのいずれかを使用するか、特定の要件に合致した情報のみを表示するカスタム ワークフローを作成することができます。

セキュリティ インテリジェンス イベントは Protectionライセンスを必要とし、表形式でのみ表示されます。セキュリティ インテリジェンス データは、シリーズ 2 の管理対象デバイスおよび DC500 防御センターではサポートされていません。セキュリティ インテリジェンス イベントからデータ グラフは作成できません。ただし、対応する接続イベントはグラフ形式で表示できます。セキュリティ インテリジェンス データのインタラクティブなグラフ表示を行うには、コンテキスト エクスプローラの [Security Intelligence] セクションを参照します。詳細については、「[Security Intelligence] セクションについて」（P.4-15）を参照してください。

各テーブル ビューまたはグラフには、表示している接続または接続サマリーについて、タイムスタンプ、IP アドレス、アプリケーションなどの情報が含まれています。FireSIGHT システムによって検出された個別の接続について利用可能な情報は、検出方法やロギング オプションなどの複数の要因によって異なります。詳細については、「接続およびセキュリティ インテリジェンスのデータ フィールド」（P.16-5）および「接続およびセキュリティ インテリジェンスのイベントで利用可能な情報」（P.16-11）を参照してください。

ヒント　[Connection Summary] ダッシュボードは、システムによってロギングされた接続の概要ビューを表示します。[Summary Dashboard] は、セキュリティ インテリジェンス イベントのデータを表示します。詳細については、「ダッシュボードの使用」（P.3-1）を参照してください。

接続またはセキュリティ インテリジェンスのデータを表示するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　次の 2 つのオプションから選択できます。

- 接続イベントを表示するには、[Analysis] > [Connections] > [Events] を選択します。
- セキュリティ インテリジェンス イベントを表示するには、[Analysis] > [Connections] > [Security Intelligence Events] を選択します。

デフォルトの接続またはセキュリティ インテリジェンスのワークフローの最初のページが表示されます。接続イベントの場合は 2 通りの可能性があります。

- ワークフローのページに**グラフ**が表示される。実行できるアクションについては、「接続グラフの使用」（P.16-16）を参照してください。
- ワークフローのページに**表**が表示される。実行できるアクションについては、「接続およびセキュリティ インテリジェンスのデータ テーブルの使用」（P.16-27）を参照してください。

セキュリティ インテリジェンス イベントの場合、ワークフローのページには**表**が表示されます。

カスタム・ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、「イベント ビュー設定の設定」（P.58-3）を参照してください。イベントが表示されない場合、時間範囲を調整する必要がある場合があります。「イベント時間の制約の設定」（P.47-27）を参照してください。

接続グラフの使用

ライセンス：任意

システムが接続データを表示する方法の 1 つがグラフです。折れ線グラフ、棒グラフ、円グラフという、3 つの接続グラフがあります。棒グラフおよび折れ線グラフは複数のデータセットを表示できます。つまり、各 X 軸データ ポイントに対し、Y 軸に複数の値を表示できます。

次のようにさまざまな方法で接続グラフを操作できます。

- グラフに表示するデータのタイプを変更する
- グラフ タイプを切り替える
- グラフを制約して、特定の時間範囲、ホスト、アプリケーション、ポート、デバイスのデータを表示します

トラフィック プロファイルは接続データに基づいているため（「トラフィック プロファイルの作成」（P.40-1）を参照）、トラフィック プロファイルは折れ線グラフとして表示できます。その他の接続グラフと同様にこれらのグラフを操作できますが、いくつかの制限があります。

セキュリティ インテリジェンス イベントからデータ グラフは作成できません。ただし、対応する接続イベントはグラフ形式で表示できます。セキュリティ インテリジェンス データのインタラクティブなグラフ表示を行うには、コンテキスト エクスプローラの [Security Intelligence] セクションを参照します。詳細については、「[Security Intelligence] セクションについて」（P.4-15）を参照してください。

注　トラフィック プロファイルを表示するには、Administrator アクセス権が必須です。任意の Security Analyst または Administrator アクセス権で表示できるその他の接続グラフと比較してみてください。

「接続およびセキュリティ インテリジェンスのデータの表示」（P.16-14）で説明したように接続グラフを表示する場合、次の表で説明する基本的な操作を実行できます。

アクセス：Admin/Any Security Analyst

表 16-3　基本的な接続グラフ機能

目的	操作
表示されたデータについて調べる	詳細については、「接続およびセキュリティ インテリジェンスのデータ フィールド」（P.16-5）を参照してください。
日付と時刻の範囲を変更する	詳細については、「イベント時間の制約の設定」（P.47-27）を参照してください。
ホストのプロファイルを表示する	発信側または応答側別に接続データを表示するグラフで、棒グラフの棒か円グラフの扇形をクリックし、[View Host Profile] を選択します。
カスタム ワークフローなどの別のワークフローを使用する	ワークフローのタイトルの横の [(switch workflow)] をクリックします。
現在のワークフローのページ間を移動する	詳細については、「ワークフローのページの使用」（P.47-21）を参照してください。
関連付けられたイベントを表示するために、ほかのイベント ビューに移動する	詳細については、「ワークフロー間のナビゲート」（P.47-41）を参照してください。

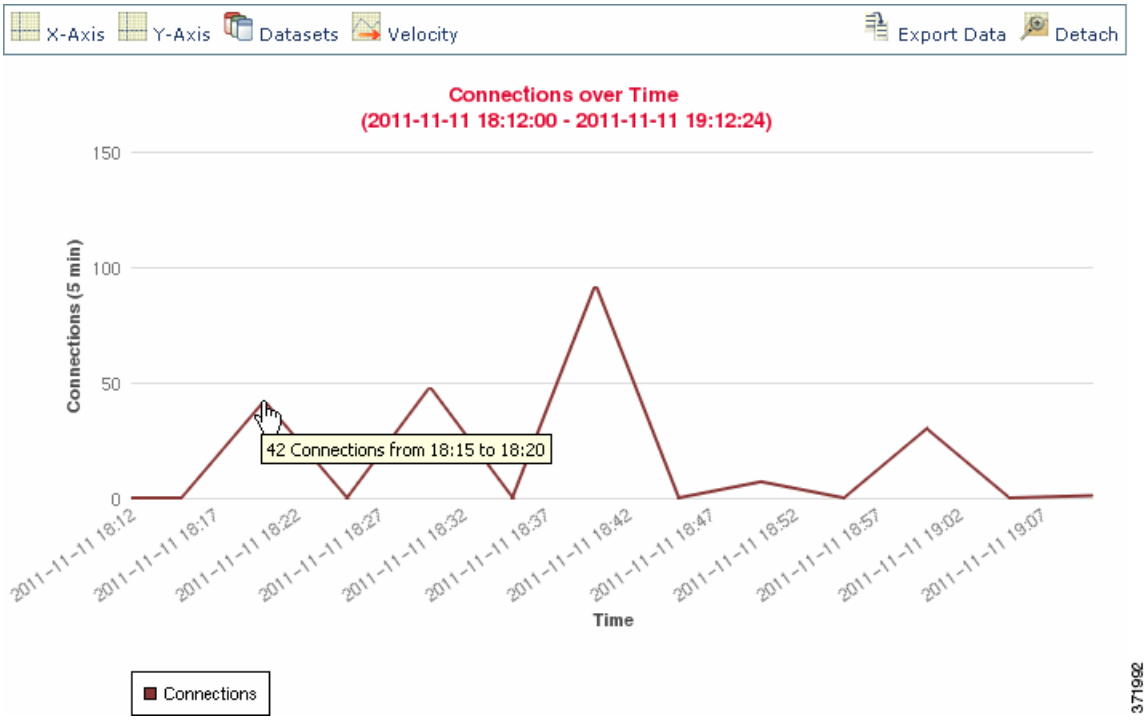
接続データの詳細な分析をする際に接続グラフを操作する方法は、ほかにも多数あります。詳細については、以下を参照してください。

- 「グラフ タイプの変更」（P.16-17）では、棒グラフと円グラフ、標準折れ線グラフと速度グラフの切り替え方法について説明しています。
- 「データシートの選択」（P.16-20）では、折れ線グラフおよび棒グラフの各 X 軸データ ポイントに対し、Y 軸に複数の値を表示する方法について説明しています。
- 「集約された接続データに関する情報の表示」（P.16-22）では、グラフ上のデータ ポイントに関する詳細情報を得る方法や、統計情報がグラフ化されているホストのプロファイルを表示する方法を説明しています。
- 「ワークロー ページでの接続グラフの操作」（P.16-23）では、ワークフローを次のページへ進めずに、接続グラフに表示されるデータを制約する方法について説明しています。
- 「接続データ グラフのドリルダウン」（P.16-23）では、ワークフローを次のページへ進めて、接続グラフに表示されるデータを制約する方法について説明しています。
- 「折れ線グラフのズームと再センタリング」（P.16-24）では、折れ線グラフを任意の時点を中心に再センタリングする方法について説明します。
- 「グラフのデータを選択する」（P.16-25）では、X 軸または Y 軸を変更することによって、接続グラフに表示されるデータを変更する方法について説明しています。
- 「接続グラフの分離」（P.16-26）では、接続グラフを新しいブラウザ ウィンドウに分離し、防御センターのデフォルトの時間範囲に影響を与えることなく詳細な分析を実行する方法について説明します。
- 「接続データのエクスポート」（P.16-27）では、グラフの作成に使用された接続データをコンマ区切り値（CSV）ファイルとしてエクスポートする方法について説明しています。

グラフ タイプの変更

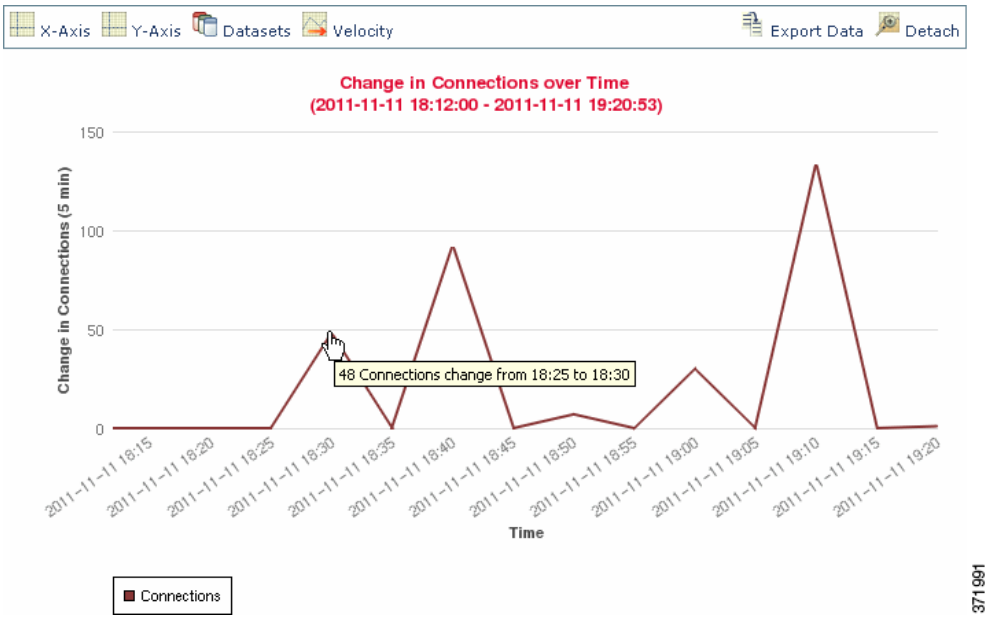
ライセンス：任意

折れ線グラフ、棒グラフ、円グラフという、3 つのタイプの接続グラフがあります。*折れ線グラフ*はある期間のデータをプロットします。たとえば次の折れ線グラフには、1 時間の時間枠において監視対象ネットワークで検出された合計接続数が表示されます。トラフィック プロファイルは常に折れ線グラフとして表示されます。

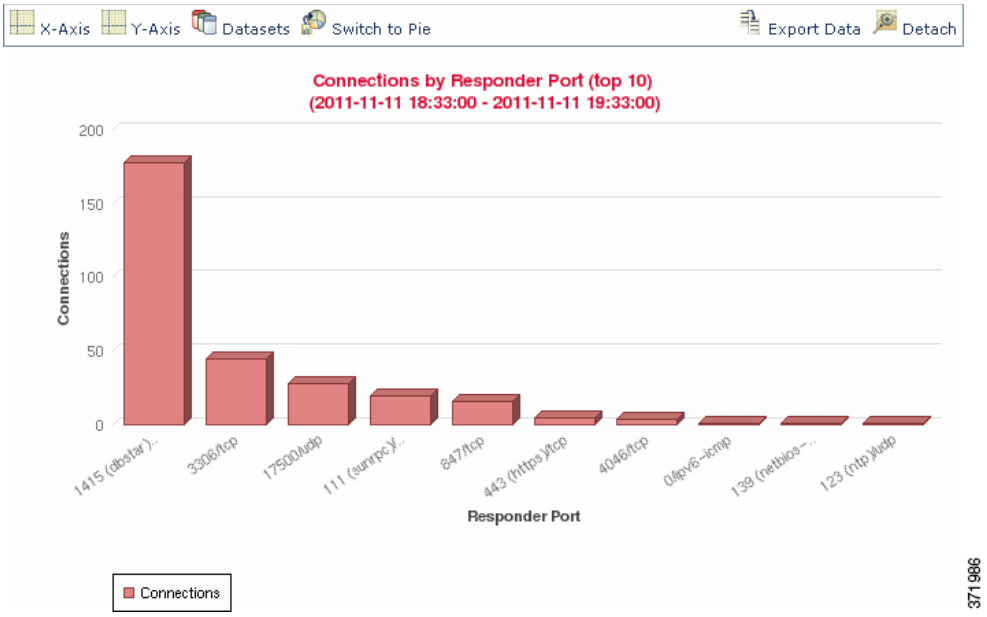


デフォルトでは、折れ線グラフは*標準ビュー*で表示されます。標準の折れ線グラフでは、5 分間隔でデータを集約し、集約したデータ ポイントをプロットし、そのポイントを接続します。

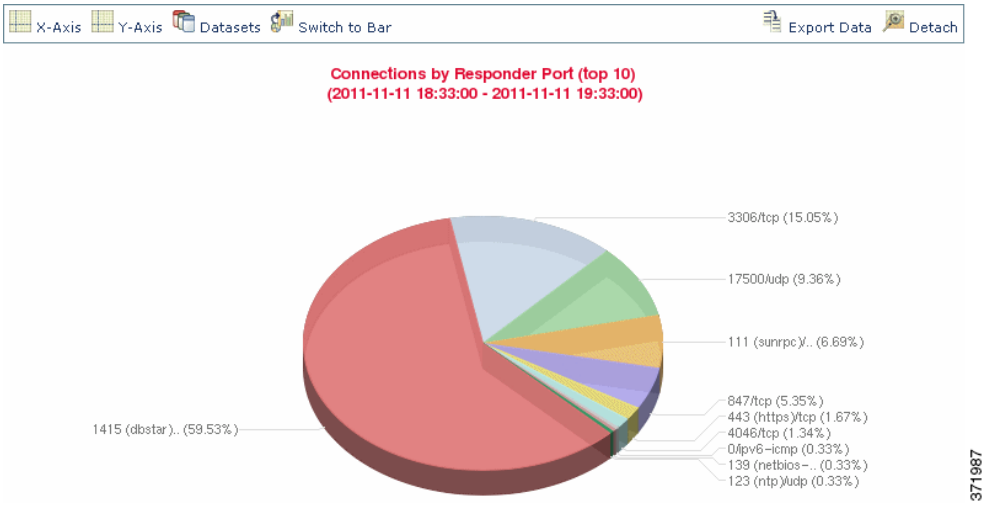
一方で、折れ線グラフは標準ビューから*速度ビュー*に変更できます。速度折れ線グラフでは、これらのデータ ポイント間の変化率を示します。上のグラフを速度グラフに変更すると、Y 軸は接続数の表示から、ある期間の接続数の変化の表示へと変わります。



*棒グラフ*は個別のカテゴリにグループ化されたデータを表示します。たとえば棒グラフは、1 時間の時間枠において最もアクティブだった 10 のポートについて、監視対象ネットワークで検出された接続数を表示できます。



*円グラフ*も棒グラフと同様に、個別のカテゴリにグループ化されたデータを表示します。次の円グラフは、前述の棒グラフと同じ情報を表示しています。



標準と速度の折れ線グラフの切り替え、棒グラフと円グラフの切り替えをするには、次の表の手順に従います。

アクセス：Admin/Any Security Analyst

表 16-4　グラフ タイプの変更

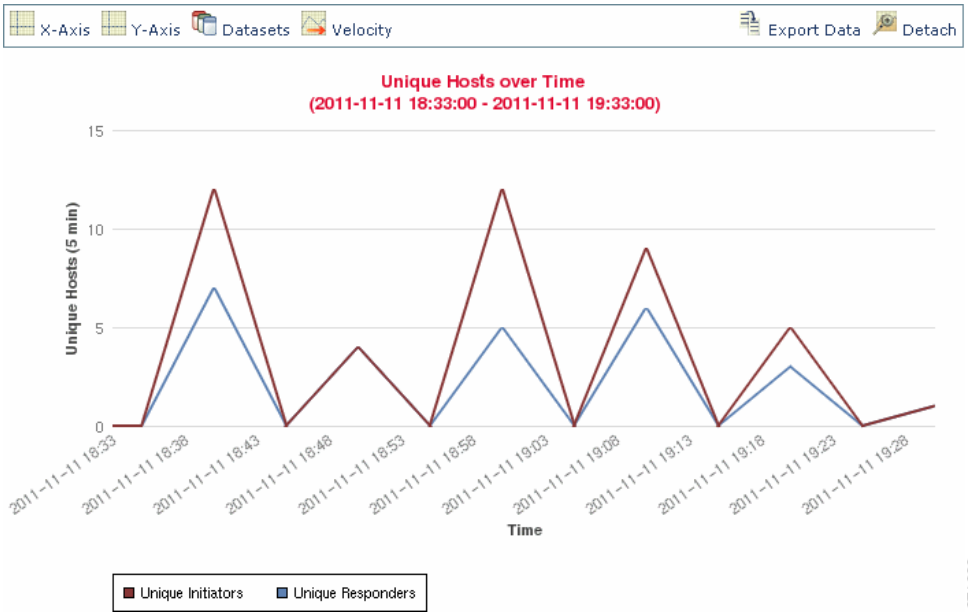
変更内容	操作
棒グラフから円グラフへ	[Switch to Pie] をクリックします。 円グラフには複数のデータセットを表示できないことに注意してください。「データシートの選択」（P.16-20）を参照してください。
円グラフから棒グラフへ	[Switch to Bar] をクリックします。
折れ線グラフを標準グラフから速度グラフへ	[Velocity] をクリックし、[Velocity] を選択します。
折れ線グラフを速度グラフから標準グラフへ	[Velocity] をクリックし、[Standard] を選択します。

データシートの選択

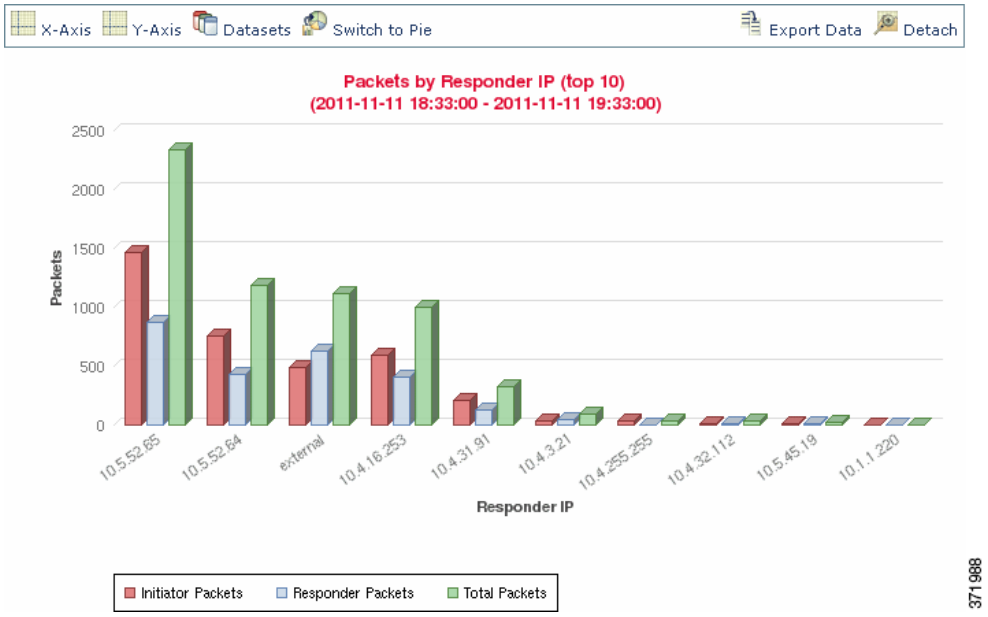
ライセンス：任意

棒グラフおよび折れ線グラフはどちらも複数のデータセットを表示できます。つまり、各 X 軸データ ポイントに対し、Y 軸に複数の値を表示できます。たとえば、一意な発信側の合計数を表示し、一意な円グラフの合計数にはデータセットを 1 つだけ表示できます。

折れ線グラフでは、複数のデータセットは複数の線として、それぞれ異なる色で表示されます。たとえば次のグラフは、監視対象ネットワークにおいて 1 時間間隔の 1 回で検出された一意な発信側の合計数と一意な応答側の合計数を表示しています。



棒グラフでは、複数のデータセットが X 軸データ ポイントごとに色分けされた棒として表示されます。たとえば次の棒グラフは、監視対象ネットワーク上で送信されたパケットの合計数と、発信側によって送信されたパケット数、応答側によって送信されたパケット数を表示しています。



円グラフには複数のデータセットを表示**できません**。複数のデータセットを持つ棒グラフから円グラフに切り替えた場合、円グラフは自動的に選択された 1 つのデータセットだけを表示します。表示するデータセットを選択する際、防御センターは、発信側と応答側の統計情報よりも全体の統計情報を優先し、応答側の統計情報よりも発信側の統計情報を優先します。次の表では、接続グラフの X 軸に表示できるデータセットについて説明します。

表 16-5　　データセットのオプション

Y 軸の表示内容	選択可能なデータセット
Connections	デフォルトの、監視対象ネットワークで検出された接続数のみ（[Connections]） これは、トラフィック プロファイル グラフの唯一のオプションです。
KBytes	以下の組み合わせ • 監視対象ネットワーク上で送信された合計キロバイト数（[Total KBytes]） • 監視対象ネットワーク上でホスト IP アドレスから送信されたキロバイト数（[Initiator KBytes]） • 監視対象ネットワーク上でホスト IP アドレスによって受信されたキロバイト数（[Responder KBytes]）
KBytes Per Second	デフォルトの、監視対象ネットワークで 1 秒あたりに送信された合計キロバイト数のみ（[Total KBytes Per Second]）

表 16-5　データセットのオプション（続き）

Y 軸の表示内容	選択可能なデータセット
Packets	以下の組み合わせ • 監視対象ネットワーク上で送信された合計パケット数（[Total Packets]） • 監視対象ネットワーク上でホスト IP アドレスから送信されたパケット数（[Initiator Packets]） • 監視対象ネットワーク上でホスト IP アドレスによって受信されたパケット数（[Responder Packets]）
Unique Hosts	以下の組み合わせ • 監視対象ネットワーク上の一意なセッション開始側の数（[Unique Initiators]） • 監視対象ネットワーク上の一意なセッション応答側の数（[Unique Responders]）
Unique Application Protocols	デフォルトの、監視対象ネットワーク上の一意なアプリケーション プロトコル数のみ（[Unique Application Protocols]）
Unique Users	デフォルトの、監視対象ネットワーク上のセッション開始側にログインした一意なユーザ数のみ（[Unique Initiator Users]）

接続グラフに表示するデータセットを選択するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　[Datasets] をクリックし、グラフに表示するデータセットを選択します。

選択できるデータセットについては、「データセットのオプション」の表で説明しています。

集約された接続データに関する情報の表示

ライセンス：任意

接続グラフは 5 分間隔で集約したデータに基づいており、*接続サマリー*とも呼ばれます。接続グラフの作成に使用された特定の接続サマリーについて、詳細情報を入手することができます。たとえば、ある期間の接続のグラフで、ある間隔に検出された正確な接続数を把握したい場合があります。

集約された接続データの詳細を取得するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　折れ線グラフの点、棒グラフの棒、もしくは円グラフの扇形の上にカーソルを置きます。グラフのその部分の作成に使用されたデータの詳細がツールチップに表示されます。

ワークロー ページでの接続グラフの操作

ライセンス：任意

接続データのワークフローを開くと、データは最初は時間範囲のみによって制約されます。ワークフローを次のページへ進めることなく、追加条件で接続グラフを制約できます。

ヒント　このように接続データを制約すると、グラフの X 軸（円グラフの表示時には独立変数とも呼びます）が変わります。接続データを制約せずに独立変数を変更するには、[X-Axis] および [Y-Axis] メニューを使用します。詳細については、「グラフのデータを選択する」（P.16-25）を参照してください。

接続データを制約するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　折れ線グラフの点、棒グラフの棒、または円グラフの扇形をクリックします。

ステップ 2　[View by...] オプションを選択します。

「X 軸の機能」の表に表示された条件のいずれかに基づいて接続データを制約できます。

たとえば、ある期間の接続のグラフについて考えてみましょう。グラフ上の点をポートによって制約すると、検出された接続イベント数に基づいて、最もアクティブだった 10 のポートを示す棒グラフが表示されますが、クリックした点を中心とする 10 分間の時間枠によって制約されます。

棒の 1 つをクリックし、[View by Initiator IP] を選択してグラフをさらに制約すると、それまでと同じ 10 分間の時間枠だけでなく、クリックした棒が表すポートでも制約された新しい棒グラフが表示されます。

注　分離したグラフを使用している場合を除いて、このように接続データを制約すると、時間範囲が変わります。分離したグラフの詳細については、「接続グラフの分離」（P.16-26）を参照してください。

接続データ グラフのドリルダウン

ライセンス：任意

接続データのワークフローを開くと、データは最初は時間範囲のみによって制約されます。ワークフローを次のページへ進めて接続グラフを制約できます。

接続データのワークフローでドリルダウンするには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　折れ線グラフの点、棒グラフの棒、または円グラフの扇形をクリックします。

ステップ 2　[Drill-down] を選択します。

次のワークフロー ページにドリルダウンし、クリックした項目を使用して制約します。

- 折れ線グラフで点をクリックすることで、次のページの時間枠は、クリックした点を中心とする 10 分間に制約されます。
- 棒グラフの棒または円グラフの扇形をクリックすると、その棒または扇形が表す条件に基づいて次のページが制約されます。たとえば、ポート使用を表す棒をクリックすると、ワークフローの次のページへドリルダウンします。これは、クリックした棒が表すポートによって制約されています。

折れ線グラフのズームと再センタリング

ライセンス：任意

折れ線グラフを任意の時点を中心に再センタリングできます。デフォルトの時間範囲を使用して再センタリングするか、別の時間範囲を選択することができます。

注　分離したグラフを使用している場合を除いて、再センタリングするとデフォルトの時間範囲が変わります。分離したグラフの詳細については、「接続グラフの分離」（P.16-26）を参照してください。

デフォルトの時間範囲を使用して再センタリングするには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　折れ線グラフ上で、グラフの再センタリングの中心にしたい点をクリックし、[recenter] をクリックします。

クリックした点を中心とする、デフォルトの時間範囲と同じ長さの時間枠のグラフが再描画されます。

別の時間範囲を使用して再センタリングするには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　グラフの再センタリングの中心にしたい点をクリックし、[Zoom] をクリックします。

ステップ 2　新しいグラフに時間範囲を選択します。最短は 1 時間、最長は 1 週間です。

クリックした点を中心とする、選択した時間枠のグラフが再描画されます。

グラフのデータを選択する

ライセンス：任意

X 軸または Y 軸、もしくは両方を変更することによって、接続グラフにさまざまなデータを表示できます。

円グラフでは、X 軸を変更すると独立変数が変わり、Y 軸を変更すると従属変数を変わることに注意してください。たとえば、ポートごとのキロバイト数を表示する円グラフについて考えてみましょう。この場合、X 軸は **Responder Port**、Y 軸は **KBytes** です。この円グラフは、ある間隔に監視対象ネットワークで送信されたデータの合計キロバイト数を表します。円の中の扇形は、各ポートで検出されたデータの比率を表します。グラフの X 軸を **Application Protocol** に変更すると、引き続き円グラフは送信データの合計キロバイト数を表しますが、円の中の扇形は検出された各アプリケーション プロトコルの送信データの比率を表します。

しかし、はじめの円グラフの Y 軸を **Packets** に変更すると、円グラフはある間隔に監視対象ネットワークで送信された合計パケット数を表し、円の中の扇形は各ポートで検出された合計パケット数を表します。

接続グラフの X 軸を変更するには、次の表の手順に従います。

表 16-6　　X 軸の機能

接続データのグラフ化方法	操作
監視対象ネットワークで最もアクティブだった 10 のアプリケーション プロトコル別に、検出済みの接続イベント数に基づいてグラフ化	[X-Axis] をクリックし、[Application Protocol] を選択します。
監視対象ネットワークで最もアクティブだった 10 の管理対象デバイス別に、検出済みの接続イベント数に基づいてグラフ化	[X-Axis] をクリックし、[Device] を選択します。
監視対象ネットワークで最もアクティブだった 10 のホスト IP アドレス別に、そのホスト IP アドレスが接続トランザクションを開始した接続イベント数に基づいてグラフ化	[X-Axis] をクリックし、[Initiator IP] を選択します。
監視対象ネットワークで最もアクティブだった 10 のユーザ別に、ユーザがログインしたホストが接続トランザクションを開始した接続イベント数に基づいてグラフ化	[X-Axis] をクリックし、Initiator User] を選択します。
監視対象ネットワークで最もアクティブだった 10 のホスト IP アドレス別に、そのアドレスが接続トランザクションの応答側となっていた接続イベント数に基づいてグラフ化	[X-Axis] をクリックし、[Responder IP] を選択します。
監視対象ネットワークで最もアクティブだった 10 のポート別に、ホストが接続トランザクションの応答側となっていた検出済みの接続イベント数に基づいてグラフ化	[X-Axis] をクリックし、[Responder Port] を選択します。
最もアクティブだった 10 の送信元デバイス（接続の接続データをエクスポートした NetFlow 対応デバイスを含む）と、FireSIGHT という名前の送信元デバイス別に、シスコの管理対象デバイスによって検出されたすべての接続についてグラフ化	[X-Axis] をクリックし、[Source Device] を選択します。
時間経過	[X-Axis] をクリックし、[Time] を選択します。

接続グラフの Y 軸を変更するには、次の表の手順に従います。

表 16-7　　Y 軸の機能

目的	操作
X 軸に選択した条件によって、監視対象ネットワークの接続数をグラフ化	[Y-Axis] をクリックし、[Connections] を選択します。
X 軸に選択した条件によって、監視対象ネットワークで送信された合計キロバイト数をグラフ化	[Y-Axis] をクリックし、[KBytes] を選択します。
X 軸に選択した条件によって、監視対象ネットワークで 1 秒あたりに送信された合計キロバイト数をグラフ化	[Y-Axis] をクリックし、[KBytes Per Second] を選択します。
X 軸に選択した条件によって、監視対象ネットワークで送信された合計パケット数をグラフ化	[Y-Axis] をクリックし、[Packets] を選択します。
X 軸に選択した条件によって、監視対象ネットワークで検出された一意なホスト数の合計をグラフ化	[Y-Axis] をクリックし、[Unique Hosts] を選択します。
X 軸に選択した条件によって、監視対象ネットワークで検出された一意なアプリケーション プロトコル数の合計をグラフ化	[Y-Axis] をクリックし、[Unique Application Protocols] を選択します。
X 軸に選択した条件によって、監視対象ネットワークで検出された一意なユーザ数の合計をグラフ化	[Y-Axis] をクリックし、[Unique Users] を選択します。

接続グラフの分離

ライセンス：任意

デフォルトの時間範囲に影響を与えることなく接続グラフの詳細な分析をしたい場合、グラフを新しいブラウザ ウィンドウに分離することができます。組み込みの接続グラフでできる操作と同じことが、分離した接続グラフでも、すべてできます。[Print] をクリックすれば、分離したグラフを印刷することもできます。トラフィック プロファイル グラフはデフォルトで分離したグラフであることに注意してください。

ヒント　分離したグラフを表示している場合、[New Window] をクリックすると、分離したグラフの別のコピーを新しいブラウザ ウィンドウで作成できます。分離した各グラフ上で、別々の分析ができるようになります。

グラフを分離するには、次に手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　[Detach] をクリックします。

接続データのエクスポート

ライセンス：任意

接続データをコンマ区切り値（CSV）ファイルとしてエクスポートすることで、ほかの人と容易に共有できます。

ヒント　また、グラフを右クリックし、ブラウザのプロンプトに従うことで、接続グラフの画像を保存できます。

接続データをエクスポートするには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　[Export Data] をクリックします。

ポップアップ ウィンドウが表示され、グラフのデータのテーブル ビューが示されます。

ステップ 2　[Download CSV File] をクリックし、ファイルを保存します。

接続およびセキュリティ インテリジェンスのデータ テーブルの使用

ライセンス：機能に応じて異なる

サポート対象デバイス：シリーズ 3、VirtualX-Series、ASA FirePOWER

サポート対象防御センター：任意（DC500 を除く）

FireSIGHT システムのイベント ビューアでは、接続データを表に表示できます。また、分析に関連する情報に応じてイベント ビューを操作できます。セキュリティ インテリジェンス イベントを表示すると、特定のセキュリティ インテリジェンスのレピュテーションがある接続に注目できます。（セキュリティ インテリジェンスは Protection ライセンスを必要とし、シリーズ 2 の管理対象デバイスおよび DC 500 防御センターではサポートされていません。）接続データにアクセスしたときに表示されるページはワークフローによって異なります。ワークフローとは、広範なビューから集中的なビューに移動することでイベントを評価するために使用できる一連のページです。

シスコによって提供される*接続イベント*および*セキュリティ インテリジェンス イベント*のワークフローは、接続と検出されたアプリケーションの基本情報の概要を表示します。これを使用して、イベントのテーブル ビューにドリルダウンできます。また、特定の要件に合致した情報だけを表示するカスタム ワークフローを作成できます。

イベント ビューアを使用して、次のことができます。

- イベントを検索、ソート、制約、また表示するイベントの時間範囲を変更する
- 表示されるカラムを指定する（テーブル ビューのみ）
- IP アドレスに関連付けられたホスト プロファイル、またはユーザ ID に関連付けられたユーザの詳細とホスト履歴を表示する
- 接続で検出されたファイル（マルウェア ファイルを含む）と侵入を表示する
- IP アドレスに関連付けられた地理情報を表示する

- 接続イベントの URL のフル テキストを表示する
- 同じワークフロー内の異なるワークフローのページを使用してイベントを表示する
- 別のワークフローを一緒に使用してイベントを表示する
- 特定の値に制約して、ワークフロー内のページからページへドリルダウンする
- 現在のページと制約をブックマークして、後で同じデータに戻れるようにする（データがまだ存在している前提）
- 現在の制約を使用してレポート テンプレートを作成する
- データベースからイベントを削除する
- IP アドレスのコンテキスト メニューを使用して、ホワイトリストまたはブラックリストに記載、もしくは接続に関連付けられたホストまたは IP アドレスに関するその他の情報を取得する

ドリルダウン ページで接続イベントを制約する場合、同一のイベントからのパケット数とバイト数が合計されることに注意してください。ただし、カスタム ワークフローを使用しており、ドリルダウン ページに [Count] カラムを追加していない場合、イベントは個別に表示され、パケット数とバイト数は合計されません。

次の項には、接続およびセキュリティ インテリジェンスのイベント テーブルの表示および分析についての情報が含まれています。

- 「ワークフローの概要と使用」（P.47-1）では、イベント ビューアの使用手順を詳しく説明しています。
- 「地理情報の使用」（P.47-24）では、接続およびセキュリティ インテリジェンスのイベントに関連付けられた地理情報を表示および解釈する方法について説明しています。
- 「イベント ビュー設定の設定」（P.58-3）では、接続およびセキュリティ インテリジェンスのイベントのデータを表示するデフォルトのワークフローを変更する方法について説明しています。
- 「接続およびセキュリティ インテリジェンスのデータ フィールド」（P.16-5）および「接続およびセキュリティ インテリジェンスのイベントで利用可能な情報」（P.16-11）では、接続およびセキュリティ インテリジェンスのイベントのデータに関する詳細を提供しています。
- 「Monitor ルールに関連付けられたイベントの使用」（P.16-28）では、Monitor ルールの条件を使用して接続イベントを制約する方法について説明しています。
- 「接続で検出されたファイルの表示」（P.16-29）では、接続で検出またはブロックされたファイル（マルウェア ファイルを含む）を表示する方法について説明しています。
- 「接続に関連付けられた侵入イベントの表示」（P.16-30）では、接続に関連付けられた侵入イベントを表示する方法について説明しています。

Monitor ルールに関連付けられたイベントの使用

ライセンス：任意

ロギングされた接続をイベント ビューアを使用して表示する場合、防御センターは各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 アクションとともに、各接続に一致する Monitor ルールを 8 つまで表示します。

接続が 1 つの Monitor ルールに一致した場合、防御センターは接続を処理したルールの名前を表示し、その後に Monitor ルール名を表示します。接続が複数の Monitor ルールに一致したときは、イベント ビューアは一致した Monitor ルールの数を `Default Action + 2 Monitor Rules` などと表示します。

一致した Monitor ルールを使用し、以下のいずれかを使用して接続イベント ビューを制約できます。

- 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
- 接続に一致した個々の Monitor ルール

接続イベントを Monitor ルールの一致を使用して制約するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Connections] > [Events] を選択します。

デフォルトの接続データのワークフローの最初のページが表示されます。

ステップ 2　分析に使用するワークフローを表示します。使用しているドリルダウン ページまたはテーブル ビューに、[Access Control Rule] フィールドが表示されていることを確認します。

ステップ 3　イベントをどのように制約しますか?

- 接続を処理したアクセス コントロールまたはデフォルト アクションに制約するには、ルール名または [Default Action] をクリックします。
- ロギングされた接続に一致した Monitor ルールのみに制約するには、Monitor ルール名をクリックします。
- ロギングされた接続に一致した複数の Monitor ルールのうち 1 つに制約するには、[*N* Monitor Rules] の値をクリックします。たとえば、[2 Monitor Rules] をクリックします。

  その接続イベントの [Monitor Rules] ポップアップ ウィンドウが表示され、接続に一致した最初の 8 つの Monitor ルールが示されます。接続イベントの制約に使用する Monitor ルール名をクリックします。

イベントが制約されます。ドリルダウン ページを使用している場合、イベント ビューがワークフローの次のページに進みます。

接続で検出されたファイルの表示

ライセンス：Protection または Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

1 つまたは複数のアクセス コントロール ルールにファイル ポリシーを関連付けると、システムは一致するトラフィックのファイル（マルウェアを含む）を検出できます。これらのルールによってロギングされた接続に関連付けられたファイル イベントがある場合は、イベント ビューアを使用して確認できます。

ファイル リストの代わりに、防御センターはファイル表示アイコン（  ）を [Files] カラムに表示します。アイコンの数字は、その接続で検出またはブロックされたファイル数（マルウェア ファイルを含む）を示します。アイコンをクリックしても、次のワークフロー ページにドリルダウンされたり、接続イベントが制約されたりすることはありません。代わりにポップアップ ウィンドウが表示され、接続で検出されたファイルのリストとともに、そのタイプと、該当する場合はマルウェア処理が示されます。

ポップアップ ウィンドウで、クリック操作によって次のことができます。

- ファイル表示アイコン（）をクリックして、ファイル イベントのテーブル ビューで詳細を表示
- マルウェア ファイル表示アイコン（）をクリックして、マルウェア イベントのテーブル ビューで詳細を表示
- ファイル軌跡アイコン（）をクリックして、ネットワークを介したファイル送信をトレース
- [View File Events] または [View Malware Events] で、接続で検出されたファイルまたはネットワークベースのマルウェア イベントのすべての詳細を表示

ヒント　1 つまたは複数の接続に関連付けられたファイルまたはマルウェア イベントをすばやく表示するには、イベント ビューアでチェック ボックスを使用して接続を選択し、[Jump to] ドロップダウン リストから [Malware Events] または [File Events] を選択します。同様に、ファイルの送信に使用された接続も表示できます。詳細については、「ワークフロー間のナビゲート」（P.47-41）を参照してください。

関連付けられたイベントを表示する際、防御センターはそのイベント タイプのデフォルトのワークフローを使用します。ファイルおよびマルウェア イベントの詳細については、「ファイル イベントの操作」（P.34-8）および「マルウェア イベントの操作」（P.34-14）を参照してください。ネットワーク ファイル トラジェクトリ機能の使用の詳細については、「ネットワーク ファイル トラジェクトリの操作」（P.34-31）を参照してください。

次のように、すべてのファイルおよびマルウェア イベントが接続に関連付けられてはいないことに注意してください。

- エンドポイントベースのマルウェア イベントは、接続に関連付けられていません。これらのイベントは、ネットワーク トラフィックをインスペクションするシステムではなく、FireAMP コネクタによって生成されます。
- IMAP に対応した電子メール クライアントの多くは単一 IMAP セッションを使用し、それはユーザがアプリケーションを終了したときに終了します。長時間接続はシステムによってロギングされますが（「長時間接続」（P.16-4）を参照）、セッションでダウンロードされたファイルは、そのセッションが終了するまで接続に関連付けられません。

また、シリーズ 2 デバイスおよび DC500 防御センターはどちらもネットワークベースの高度なマルウェア対策をサポートしていないことに注意してください。

接続に関連付けられた侵入イベントの表示

ライセンス：Protection

アクセス コントロール ルールまたはデフォルト アクションに侵入ポリシーを関連付けると、システムは一致するトラフィックのエクスプロイトを検出できます。ロギングされた接続に関連付けられた侵入イベントがある場合は、イベント ビューアを使用して確認できます。

イベント リストの代わりに、防御センターは 侵入イベント表示アイコン（）を [Intrusion Events] カラムに表示します。アイコンをクリックしても、次のワークフロー ページにドリルダウンされたり、接続イベントが制約されたりすることはありません。代わりにポップアップ ウィンドウが表示され、接続に関連付けられた侵入イベントのリストとともに、優先度と影響度が示されます。

ポップアップ ウィンドウで、一覧表示されたイベントの表示アイコン（）をクリックして、パケットのビューで詳細を表示できます。また、[View Intrusion Events] をクリックして、接続に関連付けられた侵入イベントすべての詳細を表示できます。

ヒント　1 つまたは複数の接続に関連付けられた侵入イベントをすばやく表示するには、イベント ビューアでチェック ボックスを使用して接続を選択し、[Jump to] ドロップダウン リストから [Intrusion Events] を選択します。同様に、侵入イベントに関連付けられた接続も表示できます。詳細については、「ワークフロー間のナビゲート」（P.47-41）を参照してください。

関連付けられたイベントを表示する際、防御センターはデフォルトの侵入イベント ワークフローを使用します。侵入イベントの詳細については、「侵入イベントの操作」（P.18-1）を参照してください。

接続およびセキュリティ インテリジェンスのデータの検索

ライセンス：任意

防御センター の [Search] ページを使用して、特定の接続イベント、セキュリティ インテリジェンス イベント（Protection ライセンスが必要。シリーズ 2 の管理対象デバイスおよび DC500 防御センターではサポートされていません）、接続サマリーを検索し、イベント ビューアで結果を表示し、後で再利用するために検索条件を保存できます。[Custom Analysis] ダッシュボード ウィジェット、レポート テンプレート、カスタム ユーザ ロールも、保存した検索を使用できます。

システムとともに提供される、(シスコ) というラベルが付いた検索が例です。

接続グラフは接続サマリーに基づいているため、接続サマリーを制約しているのと同じ条件が接続グラフを制約します。アスタリスク（*）が付いているフィールドが、接続グラフと接続サマリーに加えて、個々の接続またはセキュリティ インテリジェンス イベントを制約しています。

無効な検索条件を使用して接続サマリーを検索し、カスタム ワークフローの接続サマリー ページを使用して結果を見る場合、無効な条件には適用不可（N/A）としてラベルが付けられ、次の図に示すように取り消し線が引かれます。

検索結果は検索対象イベントで使用可能なデータに依存することにも注意してください。つまり、使用可能なデータによっては、検索条件が適用されないことがあります。各接続データ フィールドでデータを使用できる状況については「接続およびセキュリティ インテリジェンスのイベントで利用可能な情報」（P.16-11）を参照してください。

一般的な検索構文

システムは、各検索フィールドの横に有効な構文の例を示します。検索条件を入力する場合、次の点に注意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドでカンマ区切りの列挙を使用できます。複数の条件を入力した場合、すべての条件を満たすレコードだけが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を使用できます。
- そのフィールドで情報を利用できないイベントを特定するには、フィールドに `n/a` を指定します。そのフィールドに値が入力されているイベントを特定するには、`!n/a` を使用します。
- 検索条件としてオブジェクトを使用するには、検索フィールドの横にあるオブジェクト追加アイコン（  ）をクリックします。

検索でのオブジェクト使用など検索の構文の詳細については、「イベントの検索」（P.45-1）を参照してください。

接続およびセキュリティ インテリジェンスのデータ用の特別な検索構文

上記の一般的な検索構文に加えて、次の表では接続およびセキュリティ インテリジェンスのデータ用の特別な検索構文について説明しています。

表 16-8　接続およびセキュリティ インテリジェンスのデータの特別な検索構文

検索条件	特別な構文
接続に一致する Monitor ルール	個々の Monitor ルールに一致する接続を検索するには、[Access Control Rule] 条件を使用します。 Monitor ルールに一致するトラフィックは後で必ず別のルールかデフォルト アクションによって処理されるため、アクションが [Monitor] の接続は検索できません。Monitor ルールの名前を検索すると、後で接続を処理したルールやデフォルト アクションに関係なく、その Monitor ルールに一致したすべての接続が返されます。
数値を使用した条件（[Bytes]、[Packets]、[Connections]）	数字の前に、大なり（>）、以上（>=）、小なり（<）、以下（<=）、等しい（=）を付けられます。 **ヒント**　[Connections] 条件を使用した検索で意味のある結果を表示するには、接続サマリー ページを持つカスタム ワークフローを使用する必要があります。
接続に関連付けられた**ファイル**または**侵入イベント**	接続に関連付けられたファイル、マルウェア、侵入イベントの検索に、接続やセキュリティ インテリジェンスのイベントの検索ページは使用できません。これらの関連付けられたイベントの表示の詳細については、「接続で検出されたファイルの表示」（P.16-29）および「接続に関連付けられた侵入イベントの表示」（P.16-30）を参照してください。
接続の**開始ユーザ**または **URL**	システムは部分一致を実行します。つまり、アスタリスクを使用せずに、フィールドの内容の全部または一部を検索できます。

表 16-8　接続およびセキュリティ インテリジェンスのデータの特別な検索構文（続き）

検索条件	特別な構文
トラフィックの合計（バイト数）または接続で使用された送信の**プロトコル**	これらのカラムは、テーブル ビューには表示されません。接続テーブル ビューにプロトコルまたはトラフィックの制約があるかどうかを確認するには、検索条件を展開します。 特定のプロトコルを検索するには、名前を使用するか、http://www.iana.org/assignments/protocol-numbers に記載されたプロトコルの番号を指定します。
NetFlow 接続の **TCP フラグ**	これらのフラグの、すべてではなく、*少なくとも* 1 つがある接続をすべて表示するには、コンマ区切り TCP フラグのリストを入力します。また、[Only] チェック ボックスを選択して、指定するフラグのいずれかを唯一の TCP フラグとして持つ接続を検索できます。

接続またはセキュリティ インテリジェンスのデータを検索するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　次の 2 つのオプションから選択できます。

- 接続データを検索するには、[Table] ドロップダウン リストから、[Connection Events] を選択します。
- セキュリティ インテリジェンス データを検索するには、[Table] ドロップダウン リストから、[Security Intelligence Events] を選択します。

ページが適切な制約を使用してリロードされます。

ステップ 3　オプションで、検索を保存するには、[Name] フィールドに検索の名前を入力します。

（オプション）検索を保存すると自動的に名前が作成されます。

ステップ 4　該当するフィールドに検索条件を入力します。

接続およびセキュリティ インテリジェンスのイベント テーブルのフィールドの詳細については、「接続およびセキュリティ インテリジェンスのデータ フィールド」（P.16-5）を参照してください。

ステップ 5　他のユーザがアクセスできるように検索を保存する場合、[Save As Private] チェック ボックスをオフにします。そうしない場合は、検索をプライベートとして保存するために、チェック ボックスを選択したままにします。

検索をカスタム ユーザ ロールのデータ制限として使用する場合は、**必ず**プライベート検索として保存してください。

ステップ 6　次の選択肢があります。

- 検索を開始するには、[Search] をクリックします。

  検索結果は現在の時刻範囲によって制約されて、デフォルトのマルウェア イベントのワークフローに表示されます。
- 既存の検索を変更し、その変更を保存したい場合は、[Save] をクリックします。
- 検索基準を保存する場合は、[Save as New Search] をクリックします。検索が保存されます（[Save As Private] を選択した場合は、ユーザ アカウントに関連付けられます）。

接続サマリー ページの表示

ライセンス：任意

[Connection Summary] ページは、監視対象ネットワーク上のアクティビティをさまざまな条件で整理したグラフを表示します。たとえば [Connections over Time] グラフでは、選択した間隔における監視対象ネットワーク上の接続の合計数が表示されます。

注　[Connection Summary] ページは、接続イベントの検索によって制限されたカスタム ロールを持ち、[Connection Summary] ページへの明示的なアクセスを許可されたユーザにのみ表示されます。詳細については、「制限付きユーザ アクセス プロパティについて」（P.48-58）および「カスタム ユーザ ロールの管理」（P.48-55）を参照してください。

次の表では、[Connection Summary] ページで行うことができるさまざまな操作について説明します。

表 16-9　[Connection Summary] ページでの操作

目的	操作
[Connection Summary] ページの時刻と日付の範囲を変更	詳細については、「イベント時間の制約の設定」（P.47-27）を参照してください。
接続グラフを操作	詳細については、「接続グラフの使用」（P.16-16）を参照してください。
接続グラフをページから分離	分離したいグラフの [View] をクリックします。分離したグラフの詳細については、「接続グラフの分離」（P.16-26）を参照してください。

接続グラフでできる操作と同じことが、接続サマリーのグラフでも、ほぼすべてできます。ただし、[Connection Summary] ページのグラフは集約データに基づいているため、グラフの基になっている個々の接続イベントを調べることはできません。つまり、接続サマリーのグラフから接続データのテーブル ビューにドリルダウンすることはできません。

[Connection Summary] ページを表示するには、次の手順を実行します。

アクセス：Custom

ステップ 1　[Overview] > [Summary] > [Connection Summary] を選択します。

現在の時間範囲の [Connection Summary] ページが防御センターに表示されます。

ステップ 2　[Select Device] リストから、サマリーを表示したいデバイスを選択するか、もしくはすべてのデバイスのサマリーを表示するために [All] を選択します。