
# 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

管理対象デバイスがネットワーク上でホストによって生成されたトラフィックをモニタするとき、デバイスは検出した接続のログを生成できます。アクセス コントロールおよび SSL ポリシーでさまざまな設定を行うことで、ロギングする接続の種類、接続をロギングする時期、およびデータを保存する場所をきめ細かく制御することができます。ほとんどの場合、接続の開始または終了、またはその両方で接続をロギングできます。

接続をログに記録すると、システムによって*接続イベント*が生成されます。接続がレピュテーション ベースのセキュリティ インテリジェンス機能によってブラックリスト登録（ブロック）またはモニタされる場合は、*セキュリティ インテリジェンス イベント*と呼ばれる特別な種類の接続イベントをログに記録することもできます。

*接続イベント*と呼ばれる接続ログには、検出されたセッションに関するデータが含まれています。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。アクセス コントロールに到達する前にデバイス レベルで高速パス処理される接続を除く**すべての**接続をログに記録できます。

設定するロギングに加えて、禁止されたファイル、マルウェア、または侵入の試みをシステムが検出した場合には、ほとんどの接続を自動的にログに記録します。接続イベント ストレージを完全に無効にしない限り、システムはこれらの接続終了イベントを Defense Center データベースに保存し、さらなる分析に使用します。接続ロギングの設定の詳細については、ネットワーク トラフィックの接続のロギング（38-1 ページ）を参照してください。

**（注）** アプライアンスおよびライセンスを使用して接続をログに記録できますが、個々の接続またはセキュリティ インテリジェンス イベントで利用可能な情報は、ライセンスなど複数の要因によって異なります。詳細については、接続ロギングのライセンスおよびモデル要件（38-11 ページ）を参照してください。

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。これは、FireSIGHT システム管理対象デバイスでモニタできないネットワーク上に NetFlow 対応デバイスを配置した場合に特に有効です。

**（注）** NetFlow のデータ収集はアクセス コントロ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ません。FireSIGHT システム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 Defense Center へ送信します。NetFlow レコードはセキュリティ インテリジェンス イベントを生成できず、外部サーバにも記録できません。詳細については、NetFlow について（45-18 ページ）を参照してください。

接続イベントおよびセキュリティ インテリジェンス イベントの動作の詳細については、以下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について

**ライセンス：**任意（Any）

*接続イベント*と呼ばれる接続ログには、検出されたセッションに関するデータが含まれています。個々の接続イベントで入手可能な情報はいくつかの要因に応じて異なりますが、一般的には次のものがあります。

- タイムスタンプ、送信元と宛先の IP アドレス、入出力ゾーン、接続を処理したデバイスなど、基本的な接続特性
- アプリケーション、要求される URL、または接続に関連付けられているユーザなど、システムによって検出または推測される追加の接続特性
- ポリシーがどのアクセス コントロール ルール（または他の設定）でトラフィックを処理したか、接続が許可またはブロックされているかどうか、暗号化された接続および復号化された接続に関する詳細など、接続がログに記録された理由に関するメタデータ

アクセス コントロールおよび SSL ポリシーでさまざまな設定を行うことで、ロギングする接続の種類、接続をロギングする時期、およびデータを保存する場所をきめ細かく制御することができます。アクセス コントロール ポリシーおよび SSL ポリシーが正常に処理できる任意の接続をログに記録できます。それには、特定のアプライアンス モデルまたはライセンス付与対象の機能が必要な場合があります。接続のロギングは、次の状況で有効にすることができます。

- 接続がレピュテーション ベースのセキュリティ インテリジェンス機能によってブラックリスト登録（ブロック）またはモニタされた場合
- 暗号化セッションが SSL ポリシーによって処理される場合
- 接続がアクセス コントロール ルールまたはアクセス コントロールのデフォルト アクションによって処理された場合

設定するロギングに加えて、禁止されたファイル、マルウェア、または侵入の試みをシステムが検出した場合には、ほとんどの接続を自動的にログに記録します。他のロギング設定に関係なく、システム ポリシーを使用して接続イベント ストレージを完全に無効にしない限り、システムはこれらの接続終了イベントを Defense Center データベースに保存し、さらなる分析に使用します。

また、セキュリティ インテリジェンス ロギングを有効にすると、ブラックリストの一致によって*セキュリティ インテリジェンス イベント*および接続イベントが自動的に生成されます。セキュリティ インテリジェンス イベントは特殊なタイプの接続イベントで、個別に表示および分析できるだけでなく、個別に保存およびプルーニングできます。セキュリティ インテリジェンス ブラックリスト登録の決定を含む、接続ロギングの設定の詳細については、ネットワーク トラフィックの接続のロギング（38-1 ページ）を参照してください。

ヒント　特に断りがない限り、接続イベントに関する一般情報も、セキュリティ インテリジェンス イベントに関係します。セキュリティ インテリジェンスの詳細については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録（13-1 ページ）を参照してください。

以降の項では、検出された接続に関して使用できる情報の種類の詳細について説明します。



# 接続サマリーについて

**ライセンス：**任意（Any）

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、複数の接続が以下の状態である必要があります。

- 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-enabled 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-enabled 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、サマリー内の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わけ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

**ライセンス:**任意（Any）

接続データを集約する 5 分間隔の 2 回以上にモニタ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、システムは長時間接続が開始された 5 分間隔の数のみ増加させます。

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（Any）

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 つがモニタ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（39-3 ページ）に記載された集約条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、システムは非モニタ対象ホストの 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 フィールドについて

**ライセンス:**機能に応じて異なる

**サポートされるデバイス:**機能に応じて異なる

**サポートされる防御センター:**機能に応じて異なる

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、地理位置情報、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、[セキュリティ インテリジェンスのカテゴリ（Security Intelligence Category）] の値が割り当てられている接続のみ表示されます。

（注）　個々の接続またはセキュリティ インテリジェンス イベントで利用可能な情報は、ライセンスやアプライアンス モデルなど、いくつかの要因によって異なります。詳細については、接続ロギングのライセンスおよびモデル要件（38-11 ページ）を参照してください。

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、次の項接続イベントとセキュリティ インテリジェンス イベントで利用可能な情報（39-12 ページ）を参照してください。

**アクセス コントロール ポリシー**

接続をモニタしたアクセス コントロール ポリシー。

**アクセス コントロール ルール（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 つのモニタ ルール。

接続が 1 つのモニタ ルールに一致した場合、Defense Center は接続を処理したルールの名前を表示し、その後にモニタ ルール名を表示します。接続が複数のモニタ ルールに一致した場合、イベント ビューアは一致したモニタ 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 つのモニタ 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* モニタ ルール（N Monitor Rules）] をクリックします。

**操作**

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。

- [許可（Allow）] は、明示的に許可されてユーザがバイパスする、インタラクティブにブロックされる接続を表します。
- [信頼（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、仮想デバイス、および Blue Coat X-Series 向け Cisco NGIPS 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。

  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、モニタ ルールの有無に応じて異なるイベントを生成します。モニタ 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、接続の開始および終了イベントを生成します。アクティブなモニタ 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。
- [ブロック（Block）] と [リセットしてブロック（Block with reset）] は、ブロックされた接続を表します。さらにシステムは、[ブロック（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、SSL ポリシーによってブロックされた接続、侵入ポリシーによってエクスプロイトが検出された接続、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。
- [インタラクティブ ブロック（Interactive Block）] と [リセットしてインタラクティブ ブロック（Interactive Block with reset）] は、システムがインタラクティブ ブロック 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マークします。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 [許可（Allow）] になります。
- [デフォルト アクション（Default Action）] は、デフォルト アクションによって接続が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モニタ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（モニタ以外の）アクセス コントロール ルールのアクションであるか、またはデフォルト アクションです。同様に、モニタ ルールに一致するトラフィックは常に後続のルールまたはデフォルト アクションによって処理されるため、モニタ ルールによってロギングされた接続と関連付けられたアクションが [モニタ（Monitor）] になることはありません。

**アプリケーション プロトコル**

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。

**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。詳細については、表 45-2（ 45-12 ページ）を参照してください。

**ビジネスとの関連性**

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。詳細については、表 45-2（ 45-12 ページ）を参照してください。

**大項目、タグ（アプリケーション プロトコル、クライアント、Web アプリケーション）（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、アプリケーションの特性を示す基準。詳細については、表 45-2（ 45-12 ページ）を参照してください。

**クライアントおよびクライアント バージョン（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。

**接続（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。

**メンバー数（Count）**

各行に表示される情報に一致する接続数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ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 [カウント（Count）] 列を追加しない場合、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。

**デバイス（Device）**

接続を検出した管理対象デバイス。または、NetFlow-enabled デバイスによって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。

**ファイル（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、Defense Center 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 ルックアップの性質が示されます。

DC500 Defense Center 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（39-32 ページ）を参照してください。

**最初のパケット（First Packet）または最後のパケット（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。

**HTTP リファラ（HTTP Referrer）**

接続で検出された HTTP トラフィックの要求 URL のリファラを示す HTTP リファラ（他の URL へのリンクを提供した Web サイト、他の URL からリンクをインポートした Web サイトなど）。

**入力インターフェイス（Ingress Interface）または出力インターフェイス（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。展開環境に非同期のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインターフェイス セットに属する場合があることに注意してください。

**入力セキュリティ ゾーン（Ingress Security Zone）または出力セキュリティ ゾーン（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。

**イニシエータ バイト数（Initiator Bytes）またはレスポンダ バイト数（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。

**イニシエータの国（Initiator Country）またはレスポンダの国（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 Defense Center 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。

**イニシエータ IP（Initiator IP）またはレスポンダ IP（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 アドレスの横のホスト アイコンは見た目が少し異なります。

**イニシエータ パケット（Initiator Packets）またはレスポンダ パケット（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。

**イニシエータ ユーザ（Initiator User）**

セッションの開始側にログインしていたユーザ。

**侵入イベント**

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、Defense Center は侵入イベント表示アイコン（  ）をこのフィールドに表示します。

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、接続に関連付けられた侵入イベントのリストとともに、優先順位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（39-33 ページ）を参照してください。

**IOC**

接続に関係するホストに対する侵入の痕跡(IOC)をこのイベントがトリガーしたかどうか。IOC の詳細については、侵害の兆候(痕跡)について(45-22 ページ)を参照してください。

**NetBIOS ドメイン(NetBIOS Domain)**

セッションで使用された NetBIOS ドメイン。

**NetFlow 接続先/送信元自律システム(NetFlow Destination/Source Autonomous System)**

NetFlow-enabled 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 接続先/送信元プレフィックス(NetFlow Destination/Source Prefix)**

NetFlow-enabled 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、送信元または宛先のプレフィックス マスクが追加されたもの。

**NetFlow 接続先/送信元 ToS(NetFlow Destination/Source TOS)**

NetFlow-enabled 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-enabled デバイスに入ったか、NetFlow-enabled デバイスから出たときのタイプ オブ サービス(TOS)バイトの設定。

**NetFlow SNMP 入出力(NetFlow SNMP Input/Output)**

NetFlow-enabled 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-enabled デバイスに入ったか、NetFlow-enabled 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。

**ネットワーク分析ポリシー**

イベントの生成に関連付けられているネットワーク分析ポリシー(NAP)(ある場合)。

**理由(Reason)**

次の場合に接続がロギングされた 1 つまたは複数の原因。

- [ユーザ バイパス(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のを選択したことを示します。[ユーザ バイパス(User Bypass)] の原因は必ず [許可(Allow)] のアクションと対として組み合わされます。
- [IP ブロック(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 ブロック(IP Block)] の原因は必ず [ブロック(Block)] のアクションと対として組み合わされます。
- [IP モニタ(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モニタするように設定したことを示します。
- [ファイル モニタ(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。
- [ファイル ブロック(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。[ファイル ブロック(File 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。
- [ファイル カスタム検出(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。

- [ファイル復帰許可(File Resume Allow)] は、ファイル送信がはじめに [ファイル ブロック(Block Files)] 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たことを示します。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、HTTP セッションが自動的に再開しました。この原因は、インライン構成のみで表示されることに注意してください。
- [ファイル復帰ブロック(File Resume Block)] は、ファイル送信がはじめに [ファイル検出(Detect Files)] 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たことを示します。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、HTTP セッションが自動的に停止しました。この原因は、インライン構成のみで表示されることに注意してください。
- [SSL ブロック(SSL Block)] は、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たことを示します。[SSL ブロック(SSL Block)] の原因は必ず [ブロック(Block)] のアクションとペアになります。
- [侵入ブロック(Intrusion Block)] は、接続で検出されたエクスプロイト(侵入ポリシー違反)をシステムがブロックしたか、ブロックするはずだったことを示します。[侵入ブロック(Intrusion Block)] の原因は、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(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 [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。

**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。

**セキュリティ コンテキスト(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。システムがこのフィールドにデータを設定するのは、マルチ コンテキスト モードの ASA FirePOWER デバイスだけです。

**セキュリティ インテリジェンスのカテゴリ(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またはフィード、またはインテリジェンス フィードのカテゴリのいずれかの名前にすることができます。[理由(Reason)] が [IP ブロック(IP Block)] または [IP モニタ(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、エントリに必ず理由が表示されます。詳細については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録(13-1 ページ)を参照してください。

また、DC500 Defense Center 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。

**送信元デバイス(Source Device)**

接続のデータをエクスポートした NetFlow-enabled 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。

**送信元ポート/ICMP タイプ（Source Port/ICMP Type）または宛先ポート/ICMP コード（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。

**SSL ステータス（SSL Status）**

SSL ルールに関連したアクション、デフォルトのアクション、または暗号化接続をログに記録した復号できないトラフィック アクション。

- [ブロック（Block）] および [リセットしてブロック（Block with reset）] は、ブロックされた暗号化接続を表します。
- [復号（再署名）（Decrypt (Resign)）] は、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（キーの置き換え）（Decrypt (Replace Key)）] は、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された発信接続を表します。
- [復号（既知のキー）（Decrypt (Known Key)）] は、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。
- [復号しない（Do not Decrypt）] は、システムが復号しなかった接続を表します。

システムが暗号化接続を復号できなかった場合は、実行された復号不能のトラフィック アクションと障害の理由が表示されます。たとえば、システムが不明な暗号スイートで暗号化されたトラフィックを検出し、さらにインスペクションを行わずにそのトラフィックを許可した場合、このフィールドには [復号しない（不明な暗号スイート）（Do Not Decrypt (Unknown Cipher Suite)）] が表示されます。

証明書の詳細を表示するにはロック アイコン（  ）をクリックします。詳細については、暗号化接続に関連付けられた証明書の表示（39-34 ページ）を参照してください。

**SSL 証明書ステータス（SSL Certificate Status）**

暗号化されたトラフィックが SSL ルールと一致する場合、このフィールドにはサーバ証明書のステータスが表示されます。復号できないトラフィックが SSL ルールと一致する場合、このフィールドには [Not Checked（未チェック）] と表示されます。詳細については、証明書ステータスによる暗号化トラフィックの制御（22-26 ページ）を参照してください。

**SSL フロー エラー（SSL Flow Error）**

エラーが SSL セッション中に発生した場合はエラー名および 16 進数コード。エラーが発生しない場合は [成功（Success）]。

**SSL バージョン（SSL Version）**

接続の暗号化に使用された SSL または TLS プロトコル バージョン。

**SSL 暗号スイート（SSL Cipher Suite）**

接続の暗号化に使用された暗号スイート。

**SSL ポリシー**

接続を処理した SSL ポリシー。

**SSL ルール（SSL Rule）**

接続を処理した SSL 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初のモニタ ルール。接続がモニタ ルールに一致した場合、Defense Center は接続を処理したルールの名前を表示し、その後にモニタ ルール名を表示します。

**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 ハンドシェイク時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 フロー フラグ（SSL Flow Flags）**

暗号化された接続の最初の 10 個のデバッグ レベル フラグ。すべてのフラグを表示するには、省略記号（...）をクリックします。

**SSL フロー メッセージ（SSL Flow Messages）**

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

**TCP フラグ（TCP Flags）**

接続で検出された TCP フラグ。

**時刻**

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 カテゴリ、および URL レピュテーション（URL, URL Category, and URL Reputation）**

セッション中にモニタ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。

DC500 Defense Center 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。

**ユーザ エージェント（User Agent）**

接続で検出された HTTP トラフィックから取得したユーザ エージェント アプリケーションの情報。

**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。

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 ブラウジング（Web Browsing）] と表示されます。

# 接続イベントとセキュリティ インテリジェンス 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

**サポートされるデバイス:**機能に応じて異なる

**サポートされる防御センター:**機能に応じて異なる

個別の接続、接続サマリー、またはセキュリティ インテリジェンス イベントで利用可能な情報は、複数の要因によって異なります。

### アプライアンス モデルおよびライセンス(Appliance Model and License)

アクセス コントロール ポリシーおよび SSL ポリシーが正常に処理できる任意の接続をログに記録できます。ただし、多くの機能では、ターゲット デバイスで特定のライセンス付与対象の機能を有効化する必要があり、多くの機能は一部のモデルでのみ使用可能です。

たとえば、SSL インスペクションには シリーズ 3 デバイスが必要です。他のアプライアンス モデルは暗号化されたトラフィックを検査できません。記録された接続イベントには暗号化された接続に関する情報は含まれていません。別の例として、DC500 を使用して接続イベントのジオロケーション データを表示できません。詳細については、接続ロギングのライセンスおよびモデル要件(38-11 ページ)を参照してください。

### トラフィックの特性(Traffic Characteristics)

システムは、ネットワーク トラフィック内に存在する(および検出可能な)情報だけを報告します。たとえば、イニシエータ ホストに関連付けられているユーザがいない、またはプロトコルが DNS、HTTP、または HTTPS ではない接続で検出される参照先ホストがいない可能性があります。

### 検出方法:FireSIGHT システムまたは NetFlow

TCP フラグ、NetFlow 自律システム、プレフィックス、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 トラフィックのモニタリング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、NetFlow と FireSIGHT データの違い(45-19 ページ)を参照してください。

### ロギング方法:接続の開始または終了

システムが接続を検出するとき、その接続の開始または終了(またはその両方)をログに記録できるかどうかは、システムがその接続をどのように検出して処理するように設定されているかによって異なります。接続の開始または終了のロギング(38-5 ページ)を参照してください。

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なく、セッションの暗号化に関する詳細も含まれていません。

### インスペクション方法:関連付けられている SSL ポリシー、ファイル ポリシーおよび侵入ポリシー

SSL ポリシーによって処理された暗号化接続のみが、接続ログで SSL 関連の情報を持っています。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 ルールまたはデフォルト 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:個々またはサマリー

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。

### 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 セッションのモニタ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 [理由(Reason)] があるわけではありません。これは、インタラクティブ ブロック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。理由 (Reason) (39-8 ページ) 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、[サマリー(Summary)] 列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**　接続イベントとセキュリティ インテリジェンス イベントの両方のテーブル ビューでは、各アプリケーション タイプの [カテゴリ(category)] および [タグ(tag)] フィールド、NetFlow 関連のフィールド、SSL 関連のフィールドなど、いくつかのフィールドがデフォルトで非表示になっています。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効化された列(Disabled Columns)] の下のフィールド名をクリックします。

*表 39-1　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(End) | 個別(Single) | 要約 |
| 時刻(Time) | はい | はい | いいえ | はい | いいえ | はい |
| 最初のパケット(First Packet) | はい | はい | はい | はい | はい | いいえ |
| 最後のパケット(Last Packet) | はい | はい | いいえ | はい | はい | いいえ |
| 操作(Action) | はい | いいえ | はい | はい | はい | いいえ |
| 理由(Reason) | はい | いいえ | はい | はい | はい | いいえ |
| イニシエータ IP(Initiator IP) | はい | はい | はい | はい | はい | はい |
| イニシエータの国(Initiator Country) | はい | いいえ | はい | はい | はい | はい |
| イニシエータ ユーザ(Initiator User) | はい | はい | はい | はい | はい | はい |
| レスポンダ IP(Responder IP) | はい | はい | はい | はい | はい | はい |
| レスポンダの国(Responder Country) | はい | いいえ | はい | はい | はい | はい |

*表 39-1　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（End） | 個別（Single） | 要約 |
| セキュリティ インテリジェンスのカテゴリ（Security Intelligence Category） | はい | いいえ | はい | はい | はい | いいえ |
| 入力セキュリティ ゾーン（Ingress Security Zone） | はい | いいえ | はい | はい | はい | はい |
| 出力セキュリティ ゾーン（Egress Security Zone） | はい | いいえ | はい | はい | はい | はい |
| 送信元ポート/ICMP コード（Source Port/ICMP Code） | はい | はい | はい | はい | はい | いいえ |
| 宛先ポート/ICMP タイプ（Destination Port/ICMP Type） | はい | はい | はい | はい | はい | はい |
| SSL ステータス（SSL Status） | はい | いいえ | いいえ | はい | はい | いいえ |
| SSL 証明書ステータス（SSL Certificate Status） | はい | いいえ | いいえ | はい | はい | いいえ |
| SSL バージョン（SSL Version） | はい | いいえ | いいえ | はい | はい | いいえ |
| SSL ポリシー（SSL Policy） | はい | いいえ | いいえ | はい | はい | いいえ |
| SSL ルール（SSL Rule） | はい | いいえ | いいえ | はい | はい | いいえ |
| SSL 暗号スイート（SSL Cipher Suite） | はい | いいえ | いいえ | はい | はい | いいえ |
| SSL フロー フラグ（SSL Flow Flags） | はい | いいえ | いいえ | はい | はい | いいえ |
| SSL フロー メッセージ（SSL Flow Messages） | はい | いいえ | いいえ | はい | はい | いいえ |
| アプリケーション プロトコル（Application Protocol） | はい | はい | 利用可能な場合 | はい | はい | はい |
| クライアント（Client） | はい | いいえ | 利用可能な場合 | はい | はい | いいえ |
| クライアント バージョン（Client Version） | はい | いいえ | 利用可能な場合 | はい | はい | いいえ |
| Web アプリケーション（Web Application） | はい | いいえ | 利用可能な場合 | はい | はい | いいえ |
| 大項目、タグ（アプリケーション プロトコル、クライアント、Web アプリケーション）（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 |
| アプリケーションのリスク（Application Risk） | はい | いいえ | 利用可能な場合 | はい | はい | いいえ |
| ビジネスとの関連性（Business Relevance） | はい | いいえ | 利用可能な場合 | はい | はい | いいえ |

*表 39-1　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(End) | 個別(Single) | 要約 |
| URL | はい | いいえ | 利用可能な場合 | はい | はい | いいえ |
| URL カテゴリ(URL Category) | はい | いいえ | 利用可能な場合 | はい | はい | いいえ |
| URLレピュテーション(URL Reputation) | はい | いいえ | 利用可能な場合 | はい | はい | いいえ |
| VLAN ID(Admin. VLAN ID) | はい | いいえ | はい | はい | はい | いいえ |
| 参照ホスト(Referenced Host) | はい | いいえ | いいえ | はい | はい | いいえ |
| ユーザ エージェント(User Agent) | はい | いいえ | いいえ | はい | はい | いいえ |
| HTTP リファラ(HTTP Referrer) | はい | いいえ | いいえ | はい | はい | いいえ |
| IOC | はい | いいえ | はい | はい | はい | いいえ |
| 侵入イベント(Intrusion Events) | はい | いいえ | いいえ | はい | はい | いいえ |
| ファイル(Files) | はい | いいえ | いいえ | はい | はい | いいえ |
| 侵入ポリシー(Intrusion Policy) | はい | いいえ | はい | はい | はい | いいえ |
| アクセス コントロール ポリシー(Access Control Policy) | はい | いいえ | はい | はい | はい | いいえ |
| アクセス コントロール ルール(Access Control Rule) | はい | いいえ | はい | はい | はい | いいえ |
| ネットワーク分析ポリシー(Network Analysis Policy) | はい | いいえ | はい | はい | はい | いいえ |
| デバイス(Device) | はい | はい | はい | はい | はい | はい |
| 入力インターフェイス(Ingress Interface) | はい | いいえ | はい | はい | はい | はい |
| 出力インターフェイス(Egress Interface) | はい | いいえ | はい | はい | はい | はい |
| セキュリティ コンテキスト(ASA のみ)(Security Context (ASA only)) | はい | いいえ | はい | はい | はい | はい |
| TCP フラグ(TCP Flags) | いいえ | はい | いいえ | はい | はい | いいえ |
| NetFlow 接続先/送信元自律システム(NetFlow Destination/Source Autonomous System) | いいえ | はい | いいえ | はい | はい | いいえ |
| NetFlow 接続先/送信元プレフィックス(NetFlow Destination/Source Prefix) | いいえ | はい | いいえ | はい | はい | いいえ |
| NetFlow 接続先/送信元 ToS(NetFlow Destination/Source TOS) | いいえ | はい | いいえ | はい | はい | いいえ |

*表 39-1　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）*

| フィールド | 検出方法: | | ロギング方法: | | 接続イベント: | |
|---|---|---|---|---|---|---|
| | **FireSIGHT** | **NetFlow** | **開始** | **終了（End）** | **個別（Single）** | **要約** |
| NetFlow SNMP 入出力（NetFlow SNMP Input/Output） | いいえ | はい | いいえ | はい | はい | いいえ |
| 送信元デバイス（Source Device） | はい | はい | FireSIGHT | はい | はい | はい |
| NetBIOS ドメイン（NetBIOS Domain） | はい | いいえ | はい | はい | はい | いいえ |
| イニシエータ パケット（Initiator Packets） | はい | はい | 有用でない | はい | はい | はい |
| レスポンダ パケット（Responder Packets） | はい | はい | 有用でない | はい | はい | はい |
| イニシエータ バイト数（Initiator Bytes） | はい | はい | 有用でない | はい | はい | はい |
| レスポンダ バイト数（Responder Bytes） | はい | はい | 有用でない | はい | はい | はい |
| 接続（Connections） | はい | はい | いいえ | はい | いいえ | はい |
| メンバー数（Count） | はい | はい | はい | はい | はい | いいえ |

# 接続データとセキュリティ 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

**サポートされるデバイス:** 機能に応じて異なる

**サポートされる防御センター:** 機能に応じて異なる

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 インテリジェンスのデータは シリーズ 2 管理対象デバイスまたは DC500 Defense Center ではサポートされません。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、Context Explorer の [セキュリティ インテリジェンス（Security Intelligence）] セクションを参照します。詳細については、[セキュリティ インテリジェンス（Security Intelligence）] セクションについて（56-17 ページ）を参照してください。

**（注）** 個々の接続またはセキュリティ インテリジェンス イベントで利用可能な情報は、ライセンスやアプライアンス モデルなど、いくつかの要因によって異なります。詳細については、接続ロギングのライセンスおよびモデル要件（38-11 ページ）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で利用可能な情報は、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 フィールドについて（39-4 ページ）および接続イベントとセキュリティ インテリジェンス イベントで利用可能な情報（39-12 ページ）を参照してください。

ヒント　[接続の概要（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。[概要ダッシュボード（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（55-1 ページ）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

**手順 1**　以下の 2 つの対処法があります。

- 接続イベントを表示するには、[分析（Analysis）] > [接続（Connections）] > [イベント（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、[分析（Analysis）] > [接続（Connections）] > [セキュリティ インテリジェンス イベント（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（39-18 ページ）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（39-30 ページ）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 **（ワークフローの切り替え）** 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（71-3 ページ）を参照してください。イベントが表示されない場合は、時間範囲の調整が必要な可能性があります。イベント時間の制約の設定（58-26 ページ）を参照してください。

# 接続グラフの使用

**ライセンス：**任意（Any）

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する

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（53-1 ページ）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、Context Explorer の [セキュリティ インテリジェンス（Security Intelligence）] セクションを参照します。詳細については、[セキュリティ インテリジェンス（Security Intelligence）] セクションについて（56-17 ページ）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、管理者アクセス権が必須です。任意のセキュリティ アナリストまたは管理者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。

接続データとセキュリティ インテリジェンスのデータの表示（39-16 ページ）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 39-2　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 | 接続およびセキュリティ インテリジェンスのデータ フィールドについて（39-4 ページ） で詳細を参照してください。 |
| 時間および日付の範囲を変更する | イベント時間の制約の設定（58-26 ページ） で詳細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、[ホスト プロファイルの表示（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 [（ワークフローの切り替え）（(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 | ワークフローのページの使用（58-21 ページ） で詳細を参照してください。 |
| 他のイベント ビューに移動して関連イベントを表示する | ワークフロー間のナビゲート（58-40 ページ） で詳細を参照してください。 |

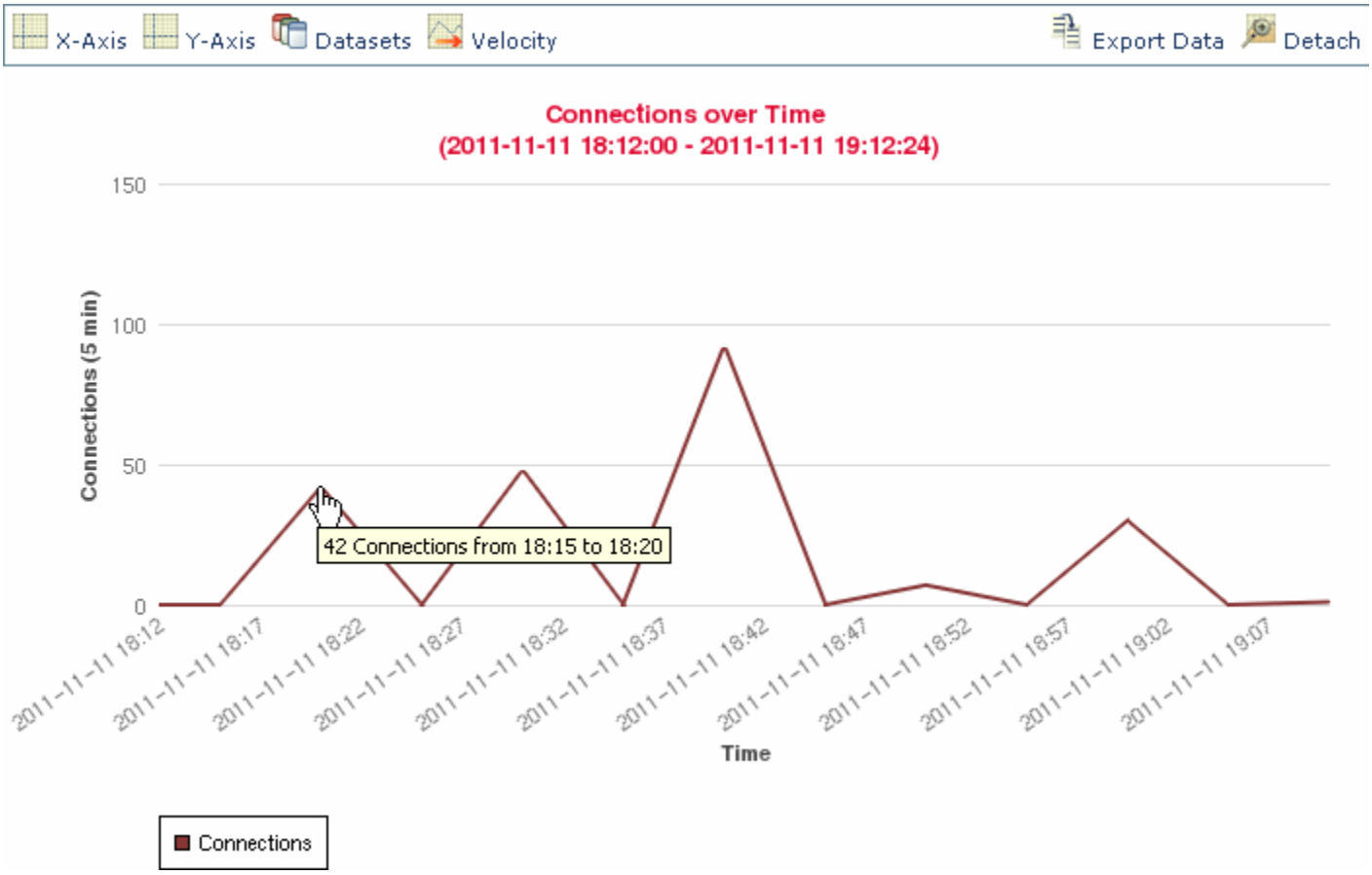
接続データの詳細な分析をする際に接続グラフを操作する方法は、ほかにも多数あります。詳細については、以下を参照してください。

- グラフ タイプの変更（39-19 ページ）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。
- データセットの選択（39-22 ページ）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（39-25 ページ）では、グラフ上のデータ ポイントに関する詳細情報を取得する方法や、統計情報がグラフ化されているホストのホスト プロファイルを表示する方法を説明しています。
- ワークフロー ページでの接続グラフの操作（39-25 ページ）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（39-26 ページ）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（39-26 ページ）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（39-27 ページ）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（39-29 ページ）では、接続グラフを新しいブラウザ ウィンドウに分離し、Defense Center 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（39-29 ページ）では、グラフの作成に使用された接続データをカンマ区切り値（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

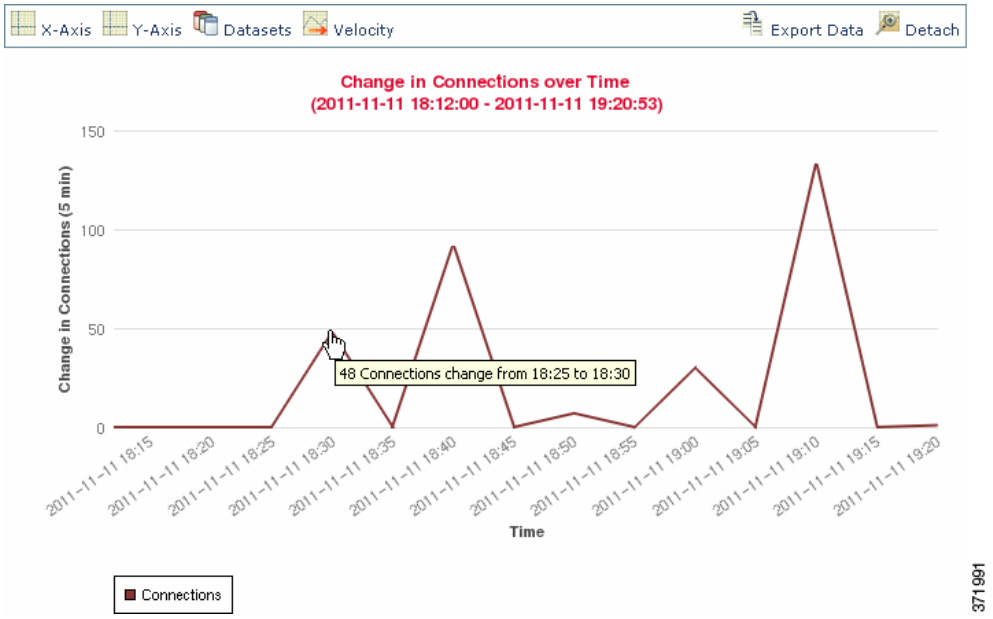
**ライセンス：**任意（Any）

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モニタ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。

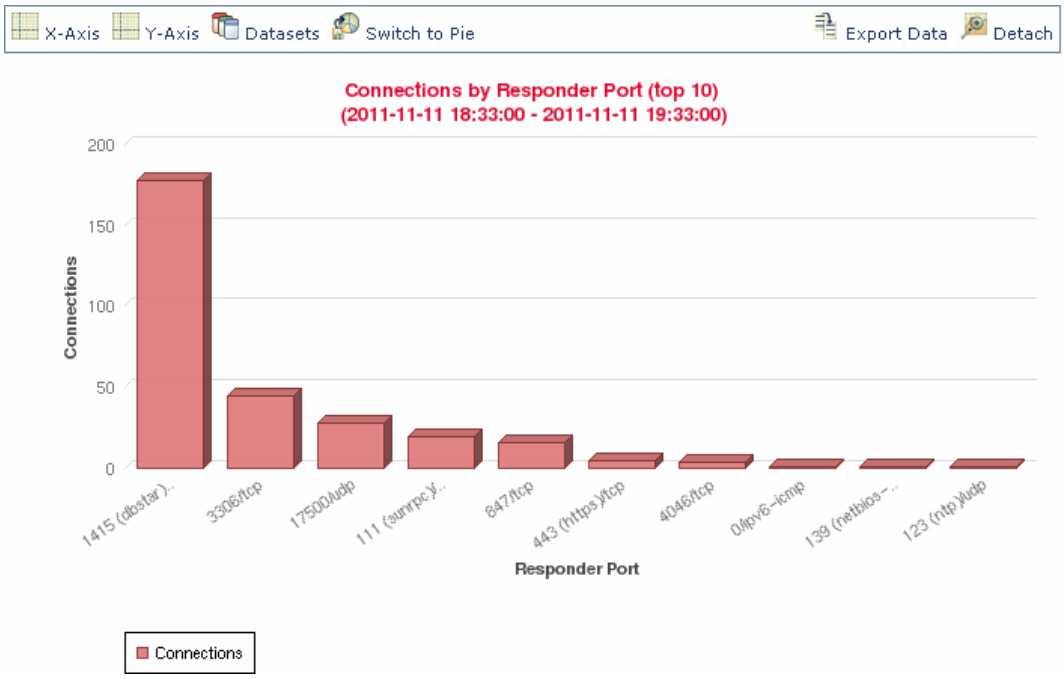



デフォルトでは、折れ線グラフは*標準ビュー*で表示されます。標準の折れ線グラフでは、5 分間隔でデータを集約し、集約データ ポイントをプロットし、そのポイントを接続します。

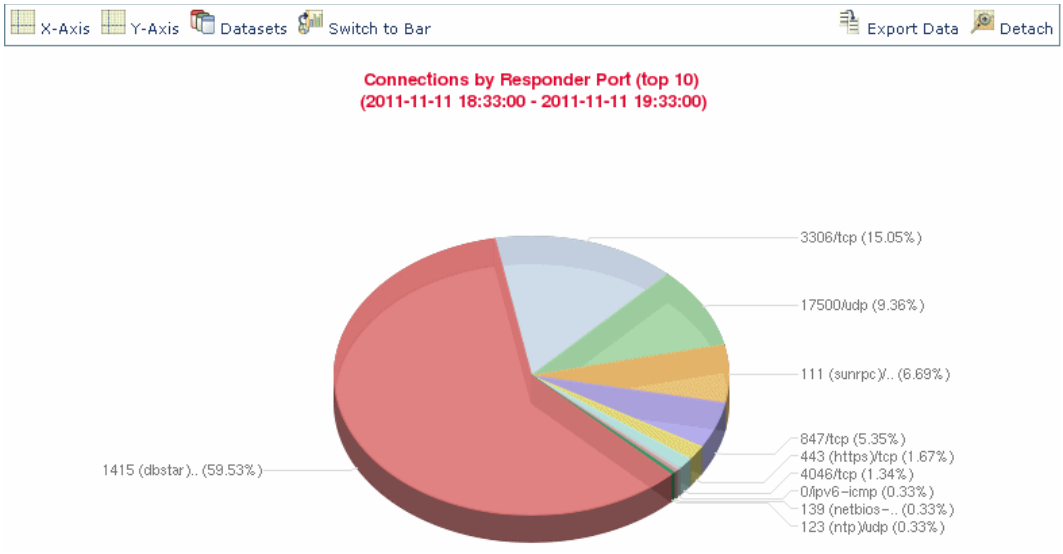
ただし、折れ線グラフは標準ビューから*速度ビュー*に変更できます。速度の折れ線グラフでは、これらのデータ ポイント間の変化のペースを示します。上のグラフを速度グラフに変更すると、Y 軸は接続数の表示から、ある期間の接続数の変化の表示へと変わります。




*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、モニタ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 39-3　　グラフ タイプの変更***

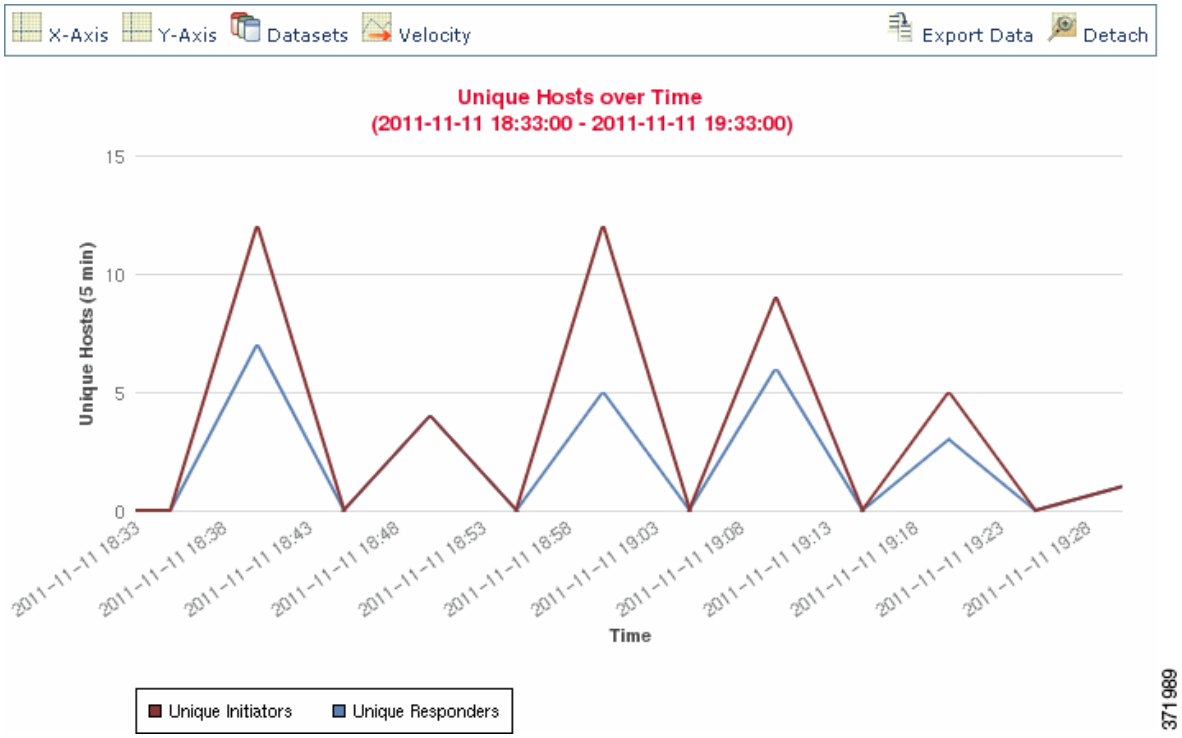
| 変更内容 | 操作 |
|---|---|
| 棒グラフから円グラフへ | [円グラフに切り替え(Switch to Pie)] をクリックします。<br>円グラフには複数のデータセットを表示できないことに注意してください。データセットの選択(39-22 ページ)を参照してください。 |
| 円グラフから棒グラフへ | [棒グラフに切り替え(Switch to Bar)] をクリックします。 |
| 折れ線グラフを標準グラフから速度グラフへ | [速度(Velocity)] をクリックし、[速度(Velocity)] を選択します。 |
| 折れ線グラフを速度グラフから標準グラフへ | [速度(Velocity)] をクリックし、[標準(Standard)] を選択します。 |

# データセットの選択

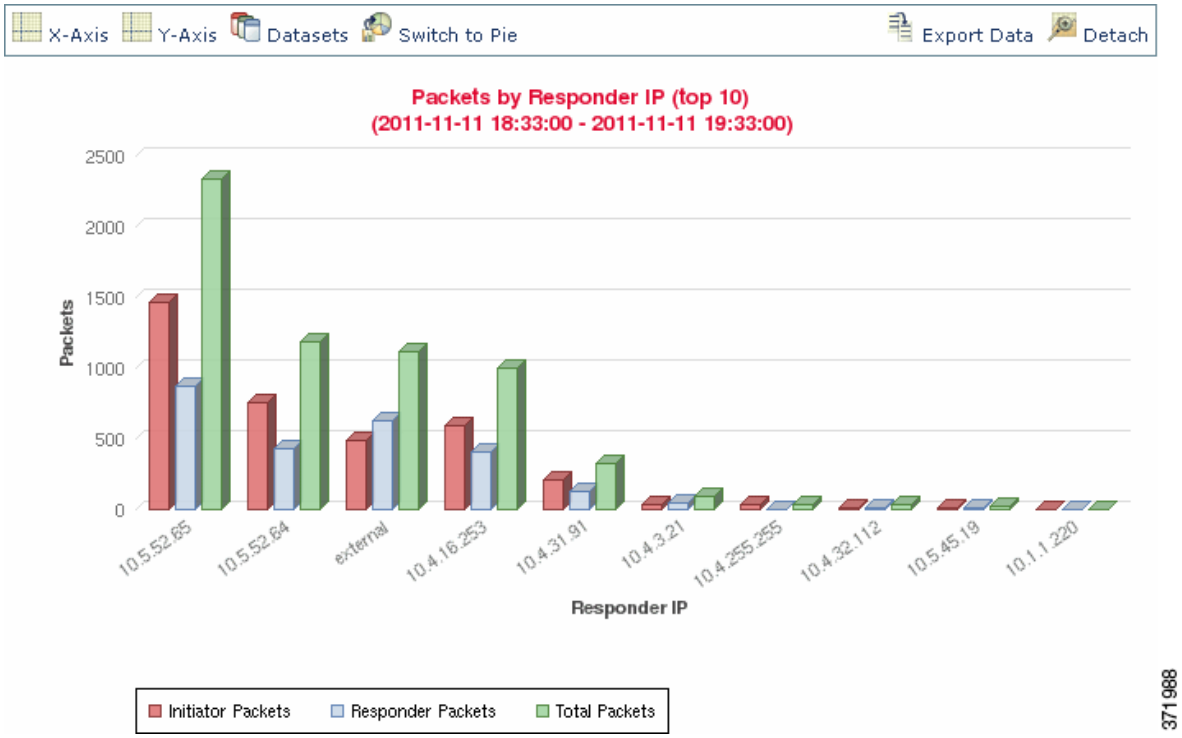
**ライセンス:**任意(Any)

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、一意のイニシエータの合計数を表示し、一意の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、モニタ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のイニシエータの合計数と一意のレスポンダ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のセットとして表示されます。たとえば次の棒グラフは、モニタ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、Defense Center 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 39-4　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 |
|---|---|
| 接続（Connections） | デフォルトの、モニタ対象ネットワークで検出された接続数のみ（[接続（Connections）]）<br>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。 |
| キロバイト数（KBytes） | 以下の組み合わせ<br>• モニタ対象ネットワーク上で送信された合計キロバイト数（[合計キロバイト数（Total KBytes）]）<br>• モニタ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（[イニシエータ キロバイト数（Initiator KBytes）]）<br>• モニタ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（[レスポンダ キロバイト数（Responder KBytes）]） |
| 1 秒あたりのキロバイト数（KBytes Per Second） | デフォルトの、モニタ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（[1 秒あたりの合計キロバイト数（Total KBytes Per Second）]） |
| パケット | 以下の組み合わせ<br>• モニタ対象ネットワーク上で送信された合計パケット数（[合計パケット（Total Packets）]）<br>• モニタ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（[イニシエータ パケット（Initiator Packets）]）<br>• モニタ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（[レスポンダ パケット（Responder Packets）]） |
| 一意のホスト（Unique Hosts） | 以下の組み合わせ<br>• モニタ対象ネットワーク上の一意のセッション開始側の数（[一意のイニシエータ（Unique Initiators）]）<br>• モニタ対象ネットワーク上の一意のセッション応答側の数（[一意のレスポンダ（Unique Responders）]） |
| 一意のアプリケーション プロトコル（Unique Application Protocols） | デフォルトの、モニタ対象ネットワーク上の一意のアプリケーション プロトコル数のみ（[一意のアプリケーションプロトコル（Unique Application Protocols）]） |
| 一意のユーザ（Unique Users） | デフォルトの、モニタ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のユーザ数のみ（[一意のイニシエータ ユーザ（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

**手順 1**　[データセット（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（Any）

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、特定の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

**手順 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。

# ワークフロー ページでの接続グラフの操作

**ライセンス：**任意（Any）

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、追加条件を指定して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ばれます）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 軸（X-Axis）] および [Y 軸（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（39-27 ページ）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

**手順 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。

**手順 2**　[表示方法（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、[発信側 IP による表示（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（39-29 ページ）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（Any）

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

**手順 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。

**手順 2**　[ドリル ダウン（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、次のページの時間範囲は、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（Any）

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（39-29 ページ）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

**手順 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、[再センタリング（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

**手順 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、[ズーム（Zoom）] をクリックします。

**手順 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（Any）

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が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 [応答側ポート（Responder Port）]、Y 軸は [キロバイト数（KBytes）] です。この円グラフは、ある間隔にモニタ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 [アプリケーション プロトコル（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。

ただし、最初の円グラフの Y 軸を [パケット（Packet）] に変更すると、円グラフはある間隔にモニタ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 39-5　　X 軸の機能***

| 接続データのグラフ化方法 | 操作 |
|---|---|
| モニタ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 軸（X-Axis）] をクリックし、[アプリケーション プロトコル（Application Protocol）] を選択します。 |
| モニタ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 軸（X-Axis）] をクリックし、[デバイス（Device）] を選択します。 |

*表 39-5　X 軸の機能（続き）*

| 接続データのグラフ化方法 | 操作 |
|---|---|
| モニタ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 軸（X-Axis）] をクリックし、[イニシエータ IP（Initiator IP）] を選択します。 |
| モニタ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 軸（X-Axis）] をクリックし、[イニシエータ ユーザ（Initiator User）] を選択します。 |
| モニタ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 軸（X-Axis）] をクリックし、[レスポンダ IP（Responder IP）] を選択します。 |
| モニタ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 軸（X-Axis）] をクリックし、[応答側ポート（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-enabled 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 軸（X-Axis）] をクリックし、[送信元デバイス（Source Device）] を選択します。 |
| 時間経過 | [X 軸（X-Axis）] をクリックし、[時間（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 39-6　Y 軸の機能*

| 目的 | 操作 |
|---|---|
| X 軸に選択した条件によって、モニタ対象ネットワークの接続数をグラフ化 | [Y 軸（Y-Axis）] をクリックし、[接続（Connections）] を選択します。 |
| X 軸に選択した条件によって、モニタ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 軸（Y-Axis）] をクリックし、[キロバイト数（KBytes）] を選択します。 |
| X 軸に選択した条件によって、モニタ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 軸（Y-Axis）] をクリックし、[1 秒あたりのキロバイト数（KBytes Per Second）] を選択します。 |
| X 軸に選択した条件によって、モニタ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 軸（Y-Axis）] をクリックし、[パケット（Packet）] を選択します。 |
| X 軸に選択した条件によって、モニタ対象ネットワークで検出された一意のホスト数の合計をグラフ化 | [Y 軸（Y-Axis）] をクリックし、[一意のホスト（Unique Hosts）] を選択します。 |
| X 軸に選択した条件によって、モニタ対象ネットワークで検出された一意のアプリケーション プロトコル数の合計をグラフ化 | [Y 軸（Y-Axis）] をクリックし、[一意のアプリケーションプロトコル（Unique Application Protocols）] を選択します。 |
| X 軸に選択した条件によって、モニタ対象ネットワークで検出された一意のユーザ数の合計をグラフ化 | [Y 軸（Y-Axis）] をクリックし、[一意のユーザ（Unique Users）] を選択します。 |

# 接続グラフの分離

**ライセンス：**任意（Any）

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。[印刷（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、[新規ウィンドウ（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

**手順 1**　[切り離し（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（Any）

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

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

**手順 1**　[データのエクスポート（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。

**手順 2**　[CSV ファイルのダウンロード（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

**サポートされるデバイス:**機能に応じて異なる

**サポートされる防御センター:**機能に応じて異なる

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 DC500 Defense Center 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。

(注)　個々の接続またはセキュリティ インテリジェンス イベントで利用可能な情報は、ライセンスやアプライアンス モデルなど、いくつかの要因によって異なります。詳細については、接続ロギングのライセンスおよびモデル要件(38-11 ページ)を参照してください。

システム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、以下を行うことができます。

- イベントの検索、ソート、および制限と、表示されるイベントの時間範囲の変更
- 表示される列の指定(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およびホスト履歴の表示
- 接続で検出されたファイル(マルウェア ファイルを含む)と侵入の表示
- IP アドレスに関連付けられた地理位置情報の表示
- 接続イベントの URL のフル テキストの表示
- セッションの暗号化に使用された証明書に関する情報の表示
- 暗号化セッションの詳細の表示
- 同じワークフロー内のさまざまなワークフロー ページを使用したイベントの表示
- 別のワークフローを使用したイベントの表示
- 特定の値で制限されるワークフロー内のページからページへのドリルダウン
- 後で同じデータに戻る(存在している場合)ための、現在のページおよび制約のブックマーク
- 現在の制約を使用したレポート テンプレートの作成
- データベースからのイベントの削除
- 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への記載、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の取得

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 [カウント(Count)] 列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。

システムが生成した接続イベントが 25 個を超えると、*接続イベント* テーブル ビューに、使用可能なイベントのページ数ではなく、[多数のうちの 1 つ(1 of Many)] と表示されます。

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(58-1 ページ)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。
- 地理位置情報の使用(58-23 ページ)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位置情報を表示および理解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(71-3 ページ)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 フィールドについて(39-4 ページ)および接続イベントとセキュリティ インテリジェンス イベントで利用可能な情報(39-12 ページ)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。
- モニタ ルールに関連付けられたイベントの使用(39-31 ページ)では、モニタ 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(39-32 ページ)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(39-33 ページ)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。
- 暗号化接続に関連付けられた証明書の表示(39-34 ページ)では、接続の暗号化に使用された証明書に関する詳細を表示する方法について説明しています。

# モニタ 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(Any)

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、Defense Center 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、各接続に一致するモニタ ルールを 8 つまで表示します。

接続が 1 つのモニタ ルールに一致した場合、Defense Center は接続を処理したルールの名前を表示し、その後にモニタ ルール名を表示します。接続が複数のモニタ ルールに一致した場合、イベント ビューアは一致したモニタ ルールの数を `Default Action + 2 Monitor Rules` などと表示します。

一致したモニタ 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モニタ ルール

**接続イベントをモニタ 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

**手順 1**　[分析(Analysis)] > [接続(Connections)] > [イベント(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。

**手順 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、[アクセス コントロール ルール(Access Control Rule)] フィールドが表示されていることを確認します。

**手順 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 ル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 [デフォルト アクション(Default Action)] をクリックします。
- ロギングされた接続に一致したモニタ ルールのみに制約するには、モニタ 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モニタ ルールのうち 1 つに制約するには、[*N* モニタ ルール(N Monitor Rules)] の値をクリックします。たとえば、[2 モニタ ルール(2 Monitor Rules)] をクリックします。

  その接続イベントの [モニタ ルール(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 つのモニタ ルールが示されます。接続イベントの制約に使用するモニタ 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またはマルウェア

**サポートされるデバイス:** 機能に応じて異なる

**サポートされる防御センター:** 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、Defense Center はファイル表示アイコン( )を [ファイル(Files)] 列に表示します。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の性質が示されます。

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 トラジェクトリ 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追跡
- [ファイル イベントの表示(View File Events)] または [マルウェア イベントの表示(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、[ジャンプ先(Jump to)] ドロップダウン リストから [マルウェア イベント(Malware Events)] または [ファイル イベント(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(58-40 ページ)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、Defense Center 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(40-8 ページ)およびマルウェア イベントの操作(40-18 ページ)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(40-39 ページ)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のみ終了します。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(39-4 ページ)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 および Blue Coat X-Series 向け Cisco NGIPS デバイスと DC500 Defense Center はどちらもネットワークベースの高度なマルウェア防御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、Defense Center は侵入イベント表示アイコン( )を [侵入イベント(Intrusion Events)] 列に表示します。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、優先順位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 ビューで詳細を表示できます。また、[侵入イベントの表示(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、[ジャンプ先（Jump to）] ドロップダウン リストから [侵入イベント（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（58-40 ページ）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、Defense Center 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（41-1 ページ）を参照してください。

# 暗号化接続に関連付けられた証明書の表示

**ライセンス：**任意（Any）

SSL インスペクションを設定すると、暗号化接続をロギングできます。トラフィックでシステムが機能し、かつ証明書が利用可能な場合は、イベント ビューアを使用して、接続の暗号化に使用された公開キー証明書の詳細を表示できます。

証明書自体の代わりに、Defense Center はロック アイコン（  ）を [SSL ステータス（SSL Status）] 列に表示します。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、次の表で説明されている証明書の詳細が示されます。

*表 39-7　暗号化接続の証明書の詳細*

| 属性 | 説明 |
|---|---|
| 件名/発行元共通名（Subject/Issuer Common Name） | 証明書のサブジェクトまたは証明書発行元のホストおよびドメイン名。 |
| 件名/発行元組織（Subject/Issuer Organization） | 証明書のサブジェクトまたは証明書発行元の組織。 |
| 件名/発行元組織ユニット（Subject/Issuer Organization Unit） | 証明書のサブジェクトまたは証明書発行元の部門。 |
| 有効期間の開始/終了（Not Valid Before/After） | 証明書の有効期間。 |
| シリアル番号（Serial Number） | 発行元 CA によって割り当てられたシリアル番号。 |
| 証明書フィンガープリント（Certificate Fingerprint） | 証明書の認証に使用する SHA ハッシュ値。 |
| 公開キー フィンガープリント（Public Key Fingerprint） | 証明書に含まれる公開キーの認証に使用する SHA ハッシュ値。 |

見出しをダブルクリックして、ポップアップ ウィンドウ内のセクションの展開または折りたたみができます。

暗号化トラフィックでシステムが機能していたが証明書が利用できない場合は、ロック アイコンがグレー表示されることに注意してください。たとえば、SSL ハンドシェイク エラーが含まれていてシステムが復号できなかった接続をシステムがブロックした場合、システムには暗号化証明書の詳細がなく、その接続のロック アイコンはグレー表示されます。

# 接続およびセキュリティ インテリジェンスのデータの検索

ライセンス：任意（Any）

Defense Center の [検索（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、または接続サマリーを検索し、その結果をイベント ビューアで表示できます。また、後で再利用するために検索条件を保存できます。カスタム分析のダッシュボード ウィジェット、レポート テンプレート、カスタム ユーザ ロールでも、保存した検索を使用できます。

サンプルとしてシステムに付属している検索には、[保存済み検索（Saved Searches）] リストで（シスコ）というラベルが付いています。

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。

無効な検索制約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表示する場合、無効な制約には適用不可（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、検索の制約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イベントとセキュリティ インテリジェンス イベントで利用可能な情報（39-12 ページ）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、次の点に留意してください。

- 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検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「A」または「B」または「C, D, E」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに A または B、または C、D、E のすべてを含むレコードが一致します。

- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 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（*）を受け入れます。
- フィールドでその情報を利用できないイベントを示すには、そのフィールドで `n/a` を指定します。フィールドに情報が入力されているイベントを示すには `!n/a` を使用します。
- 特定のデバイス、およびグループ、スタック、またはクラスタ内のデバイスを検索するには、デバイス フィールドを使用します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、検索でのデバイスの指定（60-7 ページ）を参照してください。
- 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表示されるオブジェクトの追加アイコン（ ＋ ）をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索（60-1 ページ）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、次のリスト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。

#### 接続に一致するモニタ ルール

個々のモニタ ルールに一致する接続を検索するには、[アクセス コントロール ルール（Access Control Rule）] 条件を使用します。

モニタ 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 [モニタ（Monitor）] の接続は検索できません。モニタ 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、そのモニタ 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（[バイト（Bytes）]、[パケット（Packet）]、[接続（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　[接続（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（39-32 ページ）および接続に関連付けられた侵入イベントの表示（39-33 ページ）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。

#### トラフィックの合計（バイト数）または接続で使用されたトランスポート プロトコル

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、検索制約を展開します。

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。

これらの列は、テーブル ビューには表示されません。

### 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、カンマ区切り TCP フラグのリストを入力します。また、[のみ（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。

### 接続に適用された SSL 暗号化（SSL Encryption applied to the connection）

SSL 暗号化された接続または暗号化されていない接続を表示するには、`yes` または `no` を入力します。

この列は、セキュリティ インテリジェンス イベントまたは接続イベントのテーブル ビューには表示されません。

### SSL ステータス（The SSL Status）

システムがアクションを適用した、またはシステムが条件を検出した暗号化トラフィックを表示するには、[SSL の実際の動作（SSL Actual Action）] および [SSL 障害の理由（The SSL Failure Reason）] にリストされた 1 つ以上のキーワードを入力します。このフィールドには、[SSL の実際の動作（SSL Actual Action）] の値 1 つと [SSL 障害の理由（The SSL Failure Reason）] の値 1 つを同時に含めることができます。

復号が成功すると、セキュリティ インテリジェンスおよび接続イベントのテーブル ビューには、[SSL ステータス（SSL Status）] 列に [SSL の実際の動作（SSL Actual Action）] の値が表示されます。システムがトラフィックの復号に失敗すると、セキュリティ インテリジェンスおよび接続イベントのテーブル ビューには、[SSL ステータス（SSL Status）] 列に [SSL の実際の動作（SSL Actual Action）] および [SSL 障害の理由（The SSL Failure Reason）] の両方の値が表示されます。

### 実行された実際の SSL アクション（The SSL Actual Action taken）

システムが指定したアクションを適用した暗号化されたトラフィックを表示するには、次のキーワードのいずれかを入力します。

- [復号しない（Do not Decrypt）] は、システムが復号しなかった接続を表します。
- [ブロック（Block）] および [リセットしてブロック（Block with Reset）] は、ブロックされた暗号化接続を表します。
- [復号（既知のキー）（Decrypt (Known Key)）] は、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。
- [復号（キーの置き換え）（Decrypt (Replace Key)）] は、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された発信接続を表します。
- [復号（再署名）（Decrypt (Resign)）] は、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。

復号が成功すると、セキュリティ インテリジェンスおよび接続イベントのテーブル ビューには、[SSL ステータス（SSL Status）] 列にこの値が表示されます。システムがトラフィックの復号に失敗すると、セキュリティ インテリジェンスおよび接続イベントのテーブル ビューには、[SSL ステータス（SSL Status）] 列に [SSL 障害の理由（The SSL Failure Reason）] としてこの値が表示されます。

**SSL の予期されたアクション（The SSL Expected Action）**

システムが有効な SSL ルールに指定された方法でプロセスを処理することを期待されていた、暗号化されたトラフィックを表示するには、次のキーワードのいずれかを入力します。

- [復号しない（Do not Decrypt）] は、システムが復号しなかった接続を表します。
- [ブロック（Block）] および [リセットしてブロック（Block with Reset）] は、ブロックされた暗号化接続を表します。
- [復号（既知のキー）（Decrypt (Known Key)）] は、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。
- [復号（キーの置き換え）（Decrypt (Replace Key)）] は、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された発信接続を表します。
- [復号（再署名）（Decrypt (Resign)）] は、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。

この列は、セキュリティ インテリジェンス イベントまたは接続イベントのテーブル ビューには表示されません。

**SSL 障害の理由（The SSL Failure Reason）**

システムが指定された理由で復号に失敗した暗号化トラフィックを表示するには、次のキーワードのいずれかを入力します。

- 不明（Unknown）
- 不一致（No Match）
- 成功（Success）
- キャッシュされないセッション（Uncached Session）
- 不明な暗号スイート（Unknown Cipher Suite）
- サポートされていない暗号スイート（Unsupported Cipher Suite）
- サポートされていない SSL バージョン（Unsupported SSL Version）
- SSL 圧縮の使用（SSL Compression Used）
- パッシブ モードで復号できないセッション（Session Undecryptable in Passive Mode）
- ハンドシェイク エラー（Handshake Error）
- 復号化エラー（Decryption Error）
- 保留サーバ名カテゴリ ルックアップ（Pending Server Name Category Lookup）
- 保留共通名カテゴリ ルックアップ（Pending Common Name Category Lookup）
- 内部エラー（Internal Error）
- ネットワーク パラメータを使用できません（Network Parameters Unavailable）
- 無効なサーバ証明書の処理（Invalid Server Certificate Handle）
- サーバ証明書フィンガープリントを使用できません（Server Certificate Fingerprint Unavailable）
- サブジェクト DN をキャッシュできません（Cannot Cache Subject DN）
- 発行元 DN をキャッシュできません（Cannot Cache Issuer DN）
- 不明の SSL バージョン（Unknown SSL Version）
- 外部証明書リストを使用できません（External Certificate List Unavailable）
- 外部証明書フィンガープリントを使用できません（External Certificate Fingerprint Unavailable）
- 内部証明書リストが無効です（Internal Certificate List Invalid）
- 内部証明書リストを使用できません（Internal Certificate List Unavailable）
- 内部証明書を使用できません（Internal Certificate Unavailable）

- 内部証明書フィンガープリントを使用できません(Internal Certificate Fingerprint Unavailable)
- サーバ証明書検証を使用できません(Server Certificate Fingerprint Unavailable)
- サーバ証明書検証エラー(Server Certificate Validation Failure)
- 無効なアクション(Invalid Action)

システムがトラフィックの復号に失敗すると、セキュリティ インテリジェンスおよび接続イベントのテーブル ビューには、[SSL ステータス(SSL Status)] 列に [SSL の実際の動作(SSL Actual Action)] としてこの値が表示されます。

**使用される SSL 暗号スイート(The SSL Cipher Suite used)**

接続を暗号化するのに使用される暗号スイートを表すマクロ値を入力します。暗号スイート値の指定については、www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。

**SSL 対象国(The SSL Subject Country)**

暗号化証明書の対象国に関連付けられている暗号化されたトラフィックを表示するには、2 文字の ISO 3166-1 alpha-2 国番号を入力します。

この列は、セキュリティ インテリジェンス イベントまたは接続イベントのテーブル ビューには表示されません。

**SSL 発行国(The SSL Issuer Country)**

暗号化証明書の対象国に関連付けられている暗号化されたトラフィックを表示するには、2 文字の ISO 3166-1 alpha-2 国番号を入力します。

この列は、セキュリティ インテリジェンス イベントまたは接続イベントのテーブル ビューには表示されません。

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

証明書に関連付けられているトラフィックを表示するには、その証明書の認証に使用される SHA ハッシュ値を入力するか、または貼り付けます。

この列は、セキュリティ インテリジェンス イベントまたは接続イベントのテーブル ビューには表示されません。

**SSL 公開キーのフィンガープリント(SSL Public Key Fingerprint)**

証明書に関連付けられているトラフィックを表示するには、その証明書に含まれている公開キーの認証に使用される SHA ハッシュ値を入力するか、または貼り付けます。

この列は、セキュリティ インテリジェンス イベントまたは接続イベントのテーブル ビューには表示されません。

**SSL 証明書ステータス(SSL Certificate Status)**

これは、証明書ステータスのルール条件が設定されている場合にのみ適用されます。サーバ証明書のステータスに関連付けられている暗号化されたトラフィックを表示するには、以下に示す 1 つ以上のキーワードを入力します。暗号化されたトラフィックは、複数のサーバ証明書ステータス値に同時に一致する場合があります。

- オフ(Not Checked)
- 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)

### SSL フロー メッセージ(SSL Flow Messages)

SSL ハンドシェイク時にクライアントとサーバ間で交換される次のメッセージに関連付けられている暗号化されたトラフィックを表示するには、次のキーワードのいずれかを入力します。

- HELLO_REQUEST
- CLIENT_ALERT
- SERVER_ALERT
- CLIENT_HELLO
- SERVER_HELLO
- SERVER_CERTIFICATE
- SERVER_KEY_EXCHANGE
- CERTIFICATE_REQUEST
- SERVER_HELLO_DONE
- CLIENT_CERTIFICATE
- CLIENT_KEY_EXCHANGE
- CERTIFICATE_VERIFY
- CLIENT_CHANGE_CIPHER_SPEC
- CLIENT_FINISHED
- SERVER_CHANGE_CIPHER_SPEC
- SERVER_FINISHED
- NEW_SESSION_TICKET
- HANDSHAKE_OTHER
- APP_DATA_FROM_CLIENT
- APP_DATA_FROM_SERVER

### SSL バージョン(SSL Version)

指定された SSL または TLS プロトコル バージョンに関連付けられている暗号化されたトラフィックを表示するには、次のキーワードのいずれかを入力します。

- 不明(Unknown)
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TSLv1.2

### SSL のシリアル番号(SSL Serial Number)

発行元の CA によって公開キー証明書に割り当てられたシリアル番号を入力するか、または貼り付けます。

この列は、セキュリティ インテリジェンス イベントまたは接続イベントのテーブル ビューには表示されません。

**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

**手順 1**　[分析（Analysis）] > [検索（Search）] を選択します。

[検索（Search）] ページが表示されます。

**手順 2**　次の選択肢があります。

- 接続データを検索するには、テーブルのドロップダウン リストから [接続イベント（Connection Events）] を選択します。
- 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、テーブルのドロップダウン リストから [セキュリティ インテリジェンス イベント（Security Intelligence Events）] を選択します。

ページが適切な制約によって更新されます。

**手順 3**　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 フィールドについて（39-4 ページ）を参照してください。
- 公開キー証明書に関連するフィールドの詳細については、暗号化接続に関連付けられた証明書の表示（39-34 ページ）を参照してください。
- 接続イベントおよびセキュリティ インテリジェンス イベントの特別な検索構文については、接続およびセキュリティ インテリジェンスのデータ用の特別な検索構文（39-36 ページ）を参照してください。

**手順 4**　必要に応じて検索を保存する場合は、[プライベート（Private）] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

**ヒント**　カスタム ユーザ ロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。

**手順 5**　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [保存（Save）] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存（Save）] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[プライベート（Private）] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[新規として保存（Save As New）] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存（Save）] をクリックします。検索が保存され（[プライベート（Private）] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

**手順 6**　検索を開始するには、[検索（Search）] ボタンをクリックします。

検索結果は、現在の時間範囲によって制限される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に表示されます。

# 接続サマリー ページの表示

**ライセンス：**任意（Any）

[接続の概要（Connection Summary）] ページは、モニタ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 [一定期間の接続（Connections over Time）] グラフでは、選択した間隔におけるモニタ対象ネットワーク上の接続の合計数が表示されます。

（注）　[接続の概要（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、[接続の概要（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（61-60 ページ）およびカスタム ユーザ ロールの管理（61-57 ページ）を参照してください。

次の表では、[接続の概要（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 39-8　[接続の概要（Connection Summary）] ページでの操作*

| 目的 | 操作 |
|---|---|
| [接続の概要（Connection Summary）] ページの時間と日付の範囲を変更 | イベント時間の制約の設定（58-26 ページ）で詳細を参照してください。 |
| 接続グラフを操作 | 接続グラフの使用（39-18 ページ）で詳細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 [表示（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（39-29 ページ）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、[接続の概要（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。

**[接続の概要（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：**カスタム（Custom）

**手順 1**　[概要（Overview）] > [概要（Summary）] > [接続の概要（Connection Summary）] を選択します。

現在の時間範囲の [接続の概要（Connection Summary）] ページが Defense Center に表示されます。

**手順 2**　[デバイスの選択（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、すべてのデバイスのサマリーを表示するために [すべて（All）] を選択します。