Context Explorer の使用

FireSIGHT システムContext Explorer には、モニタ対象ネットワークのステータスに関するコンテキストでの詳細でインタラクティブなグラフィカル情報が表示されます。これには、アプリケーション、アプリケーション統計、接続、位置情報、侵入の痕跡、侵入イベント、ホスト、サーバ、セキュリティ インテリジェンス、ユーザ、ファイル(マルウェア ファイルを含む)、および関連 URL に関するデータが含まれます。各セクションには、このデータが鮮やかな色の折れ線グラフ、棒グラフ、円グラフ、ドーナツ グラフの形式で表示され、グラフとともに詳しいリストが示されます。

分析を細かく調整するためのカスタム フィルタを容易に作成および適用できます。またグラフ エリアをクリックするか、カーソルをグラフ エリアに置くことで、データ セクションを詳しく調べることができます。過去 1 時間から過去 1 年までの期間を反映するように Explorer の時間範囲を設定することもできます。Context Explorer にアクセスできるユーザは、管理者、セキュリティ アナリスト、またはセキュリティ アナリスト(読み取り専用)のユーザ ロールが割り当てられているユーザだけです。

FireSIGHT システムダッシュボードは細かなカスタマイズが可能で、区分化されており、リアルタイムで更新されます。一方、Context Explorer は手動で更新され、より幅広いデータのコンテキストを提供することを目的としており、アクティブなユーザ操作のために単一で一貫性のあるレイアウトを備えています。

特定のニーズに基づいてネットワークとアプライアンスのリアルタイムのアクティビティをモニタするには、ダッシュボードを使用します。逆に、詳細かつ明確なコンテキストで事前に定義されている最新の FireSIGHT データ セットを調査するには、Context Explorer を使用します。たとえば、ネットワークのホストのうち Linux を使用しているホストは 15 % ですが、ほぼすべての YouTube トラフィックはこれらのホストによるものであることが判明した場合、Linux ホストのデータのみを表示するフィルタ、YouTube 関連のアプリケーション データのみを表示するフィルタ、あるいはこの両方のフィルタを簡単に適用できます。コンパクトで対象が絞り込まれているダッシュボード ウィジェットとは異なり、Context Explorer の各セクションは、FireSIGHT システムの専門知識を持つユーザと一般的なユーザの両方に役立つ形式で、システム アクティビティを鮮明なビジュアル表現で提供します。

表示されるデータは、管理対象デバイスのライセンスと導入方法、データを提供する機能を設定するかどうか、およびシリーズ 2アプライアンスと Blue Coat X-Series 向け Cisco NGIPS の場合はデータを提供する機能をサポートしているかどうかなどの要因に応じて異なることに注意してください。たとえば、DC500 防御センターとシリーズ 2デバイスまたは Blue Coat X-Series 向け Cisco NGIPS はいずれも、高度なマルウェア防御をサポートしていないため、DC500 防御センターはこのデータを表示できず、シリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS はこのデータを検出しません。

次の表に、ダッシュボードと Context Explorer の主な相違点の要約を示します。

表 56-1　比較：ダッシュボードおよびContext Explorer

機能	ダッシュボード	コンテキスト エクスプローラ（Context Explorer）
表示可能なデータ	FireSIGHT システムによって監視されるすべてのデータ	アプリケーション、アプリケーション統計、位置情報、侵入の痕跡、侵入イベント、ファイル（マルウェア ファイルを含む）、ホスト、セキュリティ インテリジェンス イベント、サーバ、ユーザ、および URL
カスタマイズ可能かどうか	• ダッシュボードで選択されているウィジェットはカスタマイズ可能です • 個々のウィジェットはさまざまなレベルでカスタマイズ可能です	• 基本レイアウトは変更できません • 適用されたフィルタは Explorer URL に示され、後で使用するためにブックマークできます
データの更新頻度	自動（デフォルト）、ユーザ設定	手動（Manual）
データのフィルタリング	一部のウィジェットで可能です（ウィジェット設定を編集する必要があります）	Explorer のすべての部分で可能であり、複数フィルタに対応しています
グラフィカル コンテキスト	一部のウィジェット（特に Custom Analysis）では、データをグラフ形式で表示できます。	すべてのデータの豊富なグラフィカル コンテキスト（独自の詳細なドーナツ グラフを含む）
関連 Web インターフェイス ページへのリンク	一部のウィジェット	すべてのセクション
表示データの時間範囲	ユーザ設定	ユーザ設定

関連する FireSIGHT システムダッシュボードの詳細については、ダッシュボードの使用（55-1 ページ）を参照してください。

Context Explorer について

ライセンス：FireSIGHT

Context Explorer を構成するさまざまな個別のセクションの情報から、モニタ対象ネットワークの FireSIGHT データの全体的な概要を把握できます。1 番目のセクションに表示される時間の経過に伴うトラフィックとイベント数の変化を示した折れ線グラフは、ネットワークのアクティビティにおける最近の傾向の概要を示します。

他のセクションは、侵入の痕跡、ネットワーク、アプリケーション、セキュリティ インテリジェンス、侵入、ファイル、位置情報および URL のデータをより詳細に示す一連のインタラクティブ グラフとリストからなります。トラフィックとイベントの時間グラフ以外のすべてのセクションは、表示または非表示にできます。また、すべてのセクションに表示するデータを制限するフィルタを適用できます。詳細については、Context Explorer でのフィルタの操作（56-43 ページ）を参照してください。

Context Explorer のセクションの内容と機能の詳細については、次のトピックを参照してください。

- [トラフィックと侵入イベント カウント タイム（Traffic and Intrusion Event Counts Time）] グラフについて（56-3 ページ）
- [侵入の痕跡（Indications of Compromise）] セクションについて（56-4 ページ）
- [ネットワーク情報（Network Information）] セクションについて（56-6 ページ）

- [アプリケーション情報（Application Information）] セクションについて（56-12 ページ）
- [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）
- [侵入情報（Intrusion Information）] セクションについて（56-20 ページ）
- [ファイル情報（Files Information）] セクションについて（56-26 ページ）
- [地理位置情報（Geolocation Information）] セクションについて（56-32 ページ）
- [URL 情報（URL Information）] セクションについて（56-36 ページ）

Context Explorer の設定方法全般については、次のトピックを参照してください。

- Context Explorer の更新（56-39 ページ）
- Context Explorer の時間範囲の設定（56-40 ページ）
- Context Explorer のセクションの最小化および最大化（56-40 ページ）
- Context Explorer データのドリルダウン（56-41 ページ）

Context Explorer フィルタの設定および使用方法の詳細については、次のトピックを参照してください。

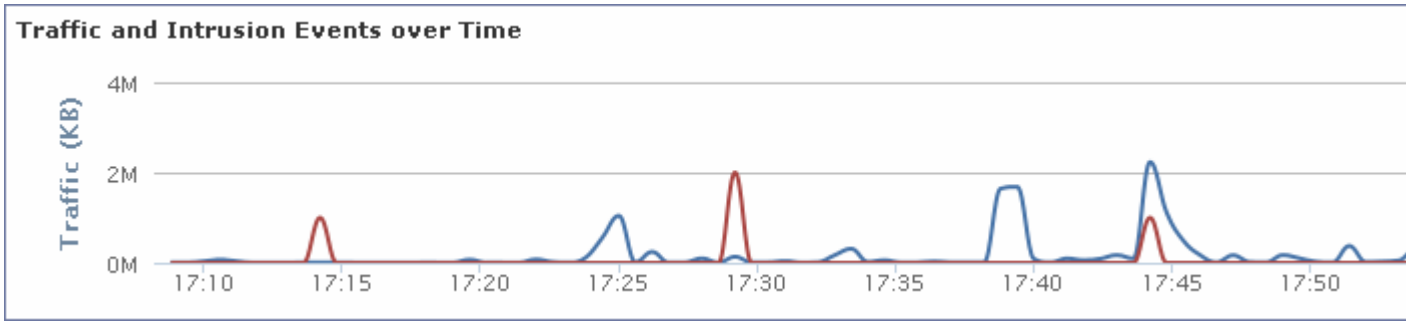
- Context Explorer でのフィルタの操作（56-43 ページ）
- フィルタの追加および適用（56-43 ページ）
- コンテキスト メニューを使用したフィルタの作成（56-47 ページ）
- フィルタのブックマーク（56-48 ページ）

[トラフィックと侵入イベント カウント タイム（Traffic and Intrusion Event Counts Time）] グラフについて

ライセンス：FireSIGHT

Context Explorer の上部には、時間の経過に伴うトラフィックおよび侵入イベント数の変化を示す折れ線グラフが表示されます。X 軸は時間間隔を示します（選択されている時間枠に応じて、5 分～ 1 か月）。Y 軸は、KB 単位のトラフィック（青色の線）と侵入イベント数（赤色の線）を示します。

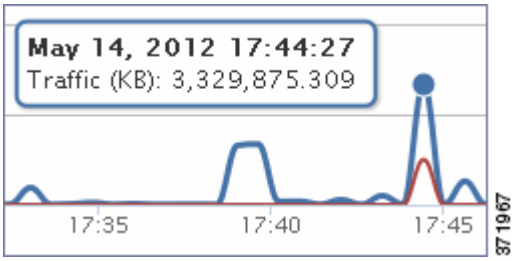
X 軸の最小間隔が 5 分であることに注意してください。これに対応するため、選択された時間範囲の開始点と終了点が、システムにより、最も近い 5 分間の間隔に調整されます。



デフォルトでは、このセクションには選択された時間範囲のすべてのネットワーク トラフィックおよび生成されたすべての侵入イベントが示されます。フィルタを適用すると、フィルタに指定されている条件に関連するトラフィックおよび侵入イベントのみがグラフに表示されます。たとえば、[OS 名（OS Name）] に `Windows` を指定してフィルタリングすると、時間グラフには Windows オペレーティング システムを使用するホストに関連するトラフィックとイベントだけが表示されます。

侵入イベント データ（[優先順位（Priority）] が `High` に設定されたものなど）に基づいて Context Explorer をフィルタリングすると、青色のトラフィックを示す線が非表示になり、侵入イベントだけに集中することができます。

トラフィックおよびイベント数に関する正確な情報を確認するには、グラフ線上の任意のポイントにポインタを置きます。色付きの線の 1 つにポインタを置くと、その線がグラフの前面に移動し、コンテキストがより明確になります。



このセクションに取り込まれるデータは主に [侵入イベント（Intrusion Events）] 表と [接続イベント（Connection Events）] 表のデータです。

[侵入の痕跡（Indications of Compromise）] セクションについて

ライセンス：FireSIGHT

Context Explorer の [侵入の痕跡（Indications of Compromise (IOC)）] セクションには、モニタ対象ネットワークでセキュリティが侵害されている可能性があるホストの概要を示す 2 つのインタラクティブ セクション（トリガーとして使用された主な IOC 種類の割合のビューと、トリガーとして使用された兆候の数をホストごとに表したビュー）が表示されます。

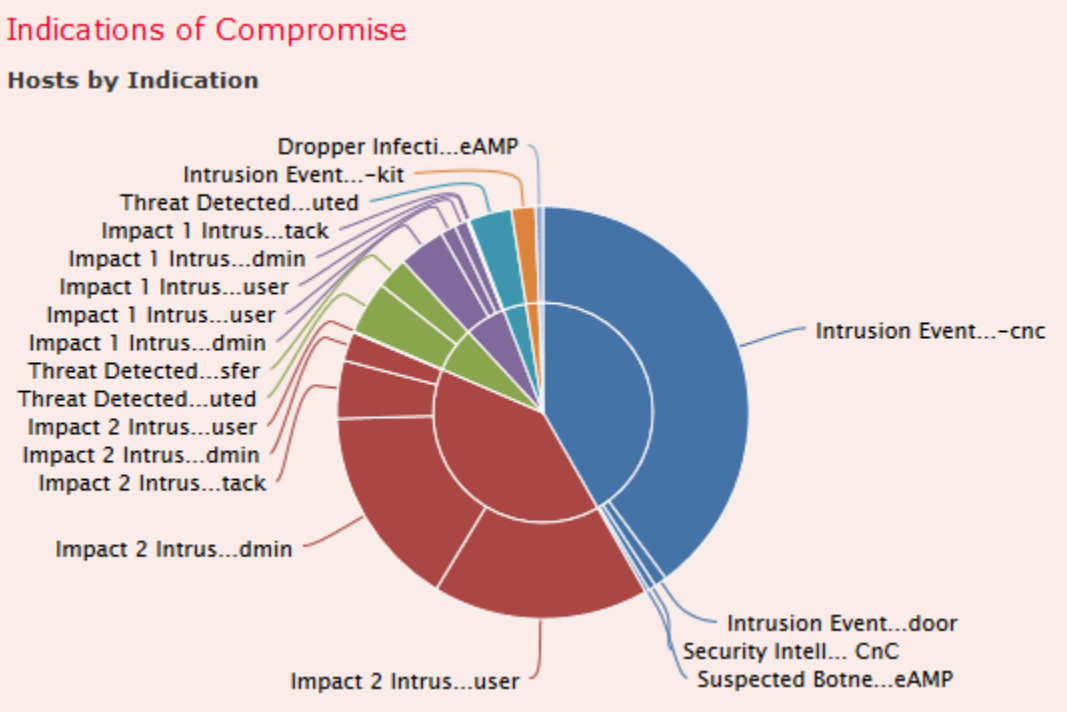
[侵入の痕跡（Indications of Compromise）] セクションのグラフの詳細については、次のトピックを参照してください。

- [痕跡別のホスト（Hosts by Indication）] グラフの表示（56-4 ページ）
- [ホスト別の痕跡（Indications by Host）] グラフの表示（56-5 ページ）

[痕跡別のホスト（Hosts by Indication）] グラフの表示

ライセンス：FireSIGHT

[痕跡別のホスト（Hosts by Indication）] グラフはドーナツ形式であり、モニタ対象ネットワーク上のホストでトリガーとして使用された侵入の痕跡（IOC）の割合のビューを表示します。内側のリングは IOC カテゴリ（`CnC Connected` や `Malware Detected` など）ごとに分割されており、外側のリングではそれがさらに具体的なイベントの種類（`Impact 2 Intrusion Event — attempted-admin` や `Threat Detected in File Transfer` など）ごとに分割されています。



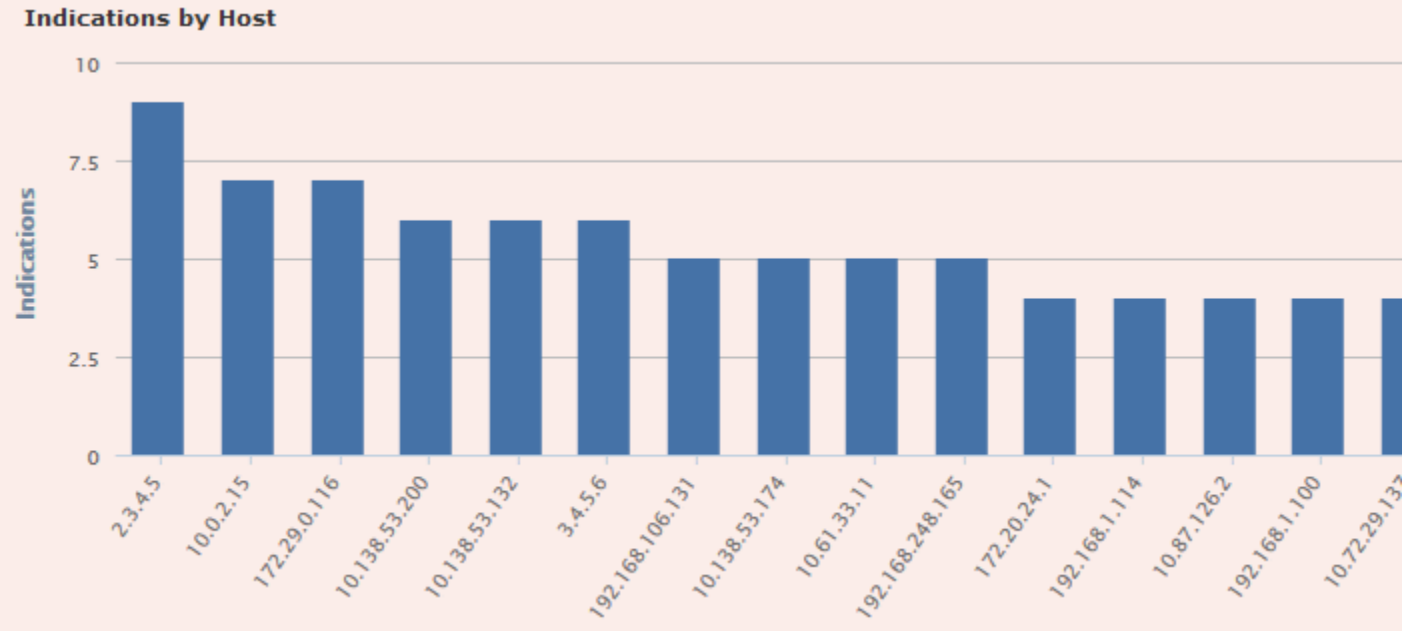
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [ホスト（Hosts）] 表と [侵入の痕跡（Indications of Compromise）] 表から取得されます。

[ホスト別の痕跡（Indications by Host）] グラフの表示

ライセンス：FireSIGHT

[ホスト別の痕跡（Indications by Host）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最も IOC が激しい 15 のホストによりトリガーとして使用された固有の侵入の痕跡（IOC）の数を表示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [ホスト（Hosts）] 表と [侵入の痕跡（Indications of Compromise）] 表から取得されます。

[ネットワーク情報（Network Information）] セクションについて

ライセンス：FireSIGHT

Context Explorer の [ネットワーク情報（Network Information）] セクションには、モニタ対象ネットワーク上の接続トラフィックの概要（トラフィックに関連する送信元、宛先、ユーザ、およびセキュリティ ゾーン、ネットワーク上のホストで使用されているオペレーティング システムの内訳、FireSIGHT システムがネットワーク トラフィックに対して実行したアクセス制御アクションの割合のビュー）を示す 6 つのインタラクティブ グラフが含まれます。

[ネットワーク情報（Network Information）] セクションのグラフの詳細については、次のトピックを参照してください。

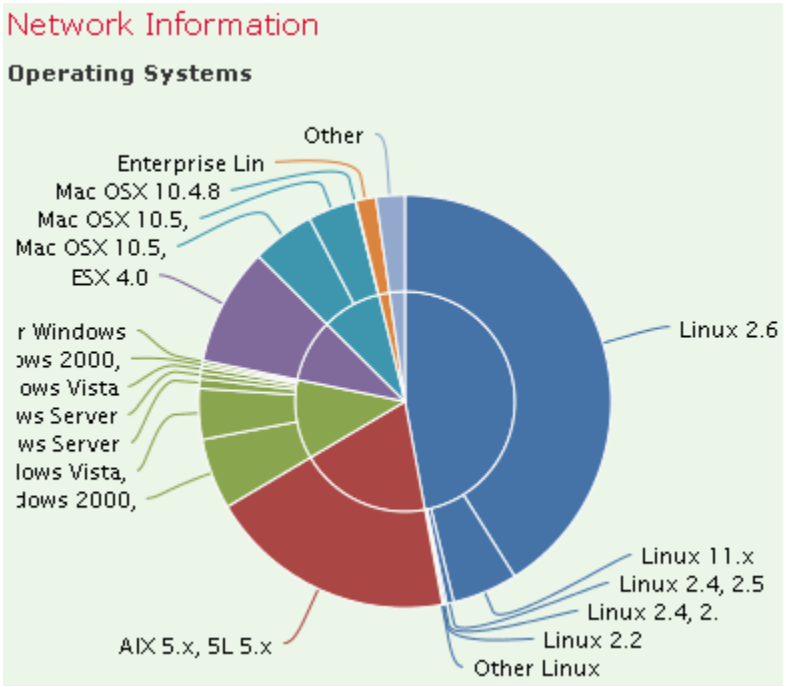
- [オペレーティング システム（Operating Systems）] グラフの表示（56-7 ページ）
- [送信元 IP 別のトラフィック（Traffic by Source IP）] グラフの表示（56-7 ページ）
- [送信元ユーザ別のトラフィック（Traffic by Source User）] グラフの表示（56-8 ページ）
- [アクセス制御アクション別の接続（Connections by Access Control Action）] グラフの表示（56-9 ページ）
- [宛先 IP 別のトラフィック（Traffic by Destination IP）] グラフの表示（56-10 ページ）
- [入力/出力セキュリティ ゾーン別のトラフィック（Traffic by Ingress/Egress Security Zone）] グラフの表示（56-11 ページ）

[オペレーティング システム（Operating Systems）] グラフの表示

ライセンス：FireSIGHT

[オペレーティング システム（Operating Systems）] グラフはドーナツ グラフ形式であり、モニタ対象ネットワークのホストで検出されたオペレーティング システムを割合で表示します。内側のリングは OS 名（Windows や Linux など）ごとに分割され、外側のリングではそのデータがさらにオペレーティング システムのバージョン（Windows Server 2008 や Linux 11.x など）ごとに分割されています。密接に関連するいくつかのオペレーティング システム（Windows 2000、Windows XP、Windows Server 2003 など）は 1 つにまとめられます。ごく少数の認識されないオペレーティング システムは [その他（Other）] にまとめられます。

このグラフは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Explorer の時間範囲を変更しても、グラフは変化しません。



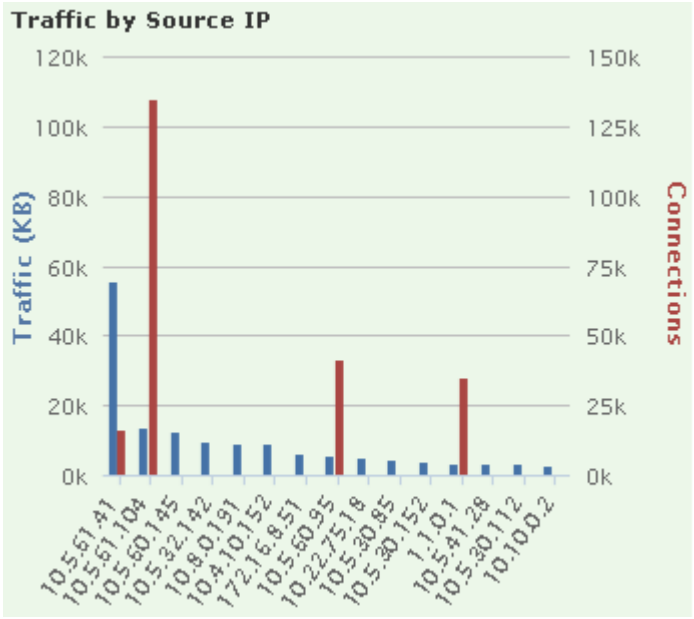
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [ホスト（Hosts）] 表から取得されます。

[送信元 IP 別のトラフィック（Traffic by Source IP）] グラフの表示

ライセンス：FireSIGHT

[送信元 IP 別のトラフィック（Traffic by Source IP）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最もアクティブな上位 15 の送信元 IP アドレスのネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされた送信元 IP アドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

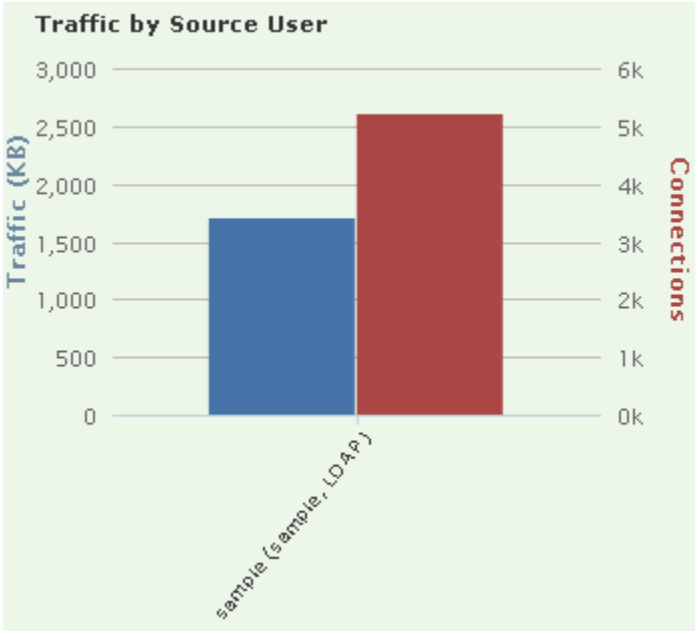
(注)　侵入イベントの情報でフィルタリングすると、[送信元 IP 別のトラフィック（Traffic by Source IP）] グラフは非表示になります。

このグラフのデータは主に [接続イベント（Connection Events）] 表から取得されます。

[送信元ユーザ別のトラフィック（Traffic by Source User）] グラフの表示

ライセンス：FireSIGHT

[送信元ユーザ別のトラフィック（Traffic by Source User）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最もアクティブな上位 15 の送信元ユーザのネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされた送信元 IP アドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

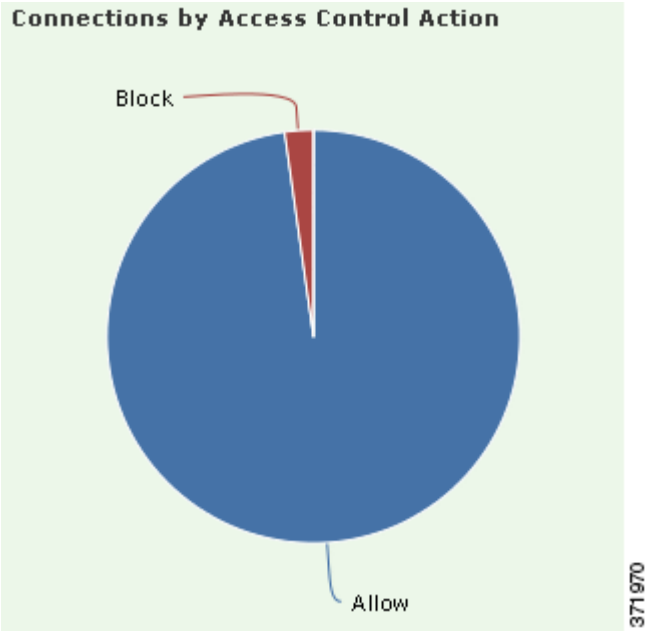
(注)　侵入イベントの情報でフィルタリングすると、[送信元ユーザ別のトラフィック(Traffic by Source User)] グラフは非表示になります。

このグラフのデータは主に [接続イベント(Connection Events)] 表から取得されます。User Agent によって報告されるユーザのみが表示されることに注意してください。

[アクセス制御アクション別の接続(Connections by Access Control Action)] グラフの表示

ライセンス:FireSIGHT

[アクセス制御アクション別の接続(Connections by Access Control Action)] グラフは円グラフ形式であり、導入されている FireSIGHT システムでモニタ対象トラフィックに対して実行されたアクセス制御アクション([ブロック(Block)] や [許可(Allow)] など)の割合のビューを表示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

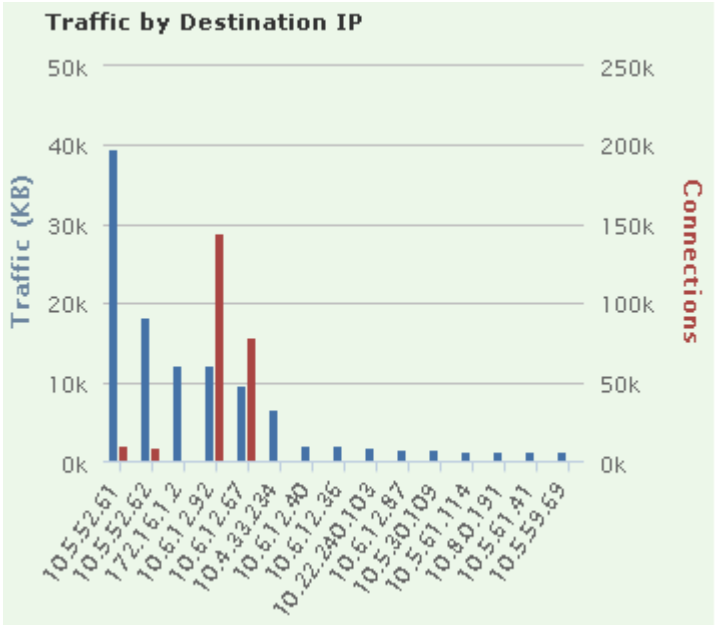
(注)　侵入イベントの情報でフィルタリングすると、[送信元ユーザ別のトラフィック（Traffic by Source User）] グラフは非表示になります。

このグラフのデータは主に [接続イベント（Connection Events）] 表から取得されます。

[宛先 IP 別のトラフィック（Traffic by Destination IP）] グラフの表示

ライセンス：FireSIGHT

[宛先 IP 別のトラフィック（Traffic by Destination IP）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最もアクティブな上位 15 の宛先 IP アドレスのネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされた宛先 IP アドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

(注)　侵入イベントの情報でフィルタリングすると、[宛先 IP 別のトラフィック（Traffic by Destination IP）] グラフは非表示になります。

このグラフのデータは主に [接続イベント（Connection Events）] 表から取得されます。

[入力/出力セキュリティ ゾーン別のトラフィック（Traffic by Ingress/Egress Security Zone）] グラフの表示

ライセンス：FireSIGHT

[入力/出力セキュリティ ゾーン別のトラフィック（Traffic by Ingress/Egress Security Zone）] グラフは棒グラフ形式であり、モニタ対象ネットワークで設定されている各セキュリティ ゾーンごとに、その着信/発信ネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。必要に応じて、このグラフに入力（デフォルト）セキュリティ ゾーン情報または出力セキュリティ ゾーン情報のいずれかを表示するように設定できます。

リストされたセキュリティ ゾーンごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。セキュリティ ゾーンの詳細については、セキュリティ ゾーンの操作（3-44 ページ）を参照してください。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、出力セキュリティ ゾーンのトラフィックのみが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [出力(Egress)] をクリックします。デフォルト ビューに戻すには [入力(Ingress)] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトの [入力(Ingress)] ビューに戻ることに注意してください。

(注)　侵入イベントの情報でフィルタリングすると、[入力/出力セキュリティ ゾーン別のトラフィック(Traffic by Ingress/Egress Security Zone)] グラフは非表示になります。

このグラフのデータは主に [接続イベント(Connection Events)] 表から取得されます。

[アプリケーション情報(Application Information)] セクションについて

ライセンス: FireSIGHT

Context Explorer の [アプリケーション情報(Application Information)] セクションには、3 つのインタラクティブ グラフと 1 つの表形式リストが表示されます。これらのグラフとリストは、モニタ対象ネットワーク上でのアプリケーション アクティビティの概要(アプリケーションに関連するトラフィック、侵入イベント、およびホストを、各アプリケーションに割り当てられている推定のリスクまたはビジネスとの関連性ごとに編成したもの)を示します。[アプリケーション詳細リスト(Application Details List)] は、各アプリケーションとそのリスク、ビジネスとの関連性、カテゴリ、およびホスト数を示すインタラクティブなリストです。

このセクションのすべての「アプリケーション」インスタンスについて、[アプリケーション情報（Application Information）] のグラフのセットは、デフォルトでは特にアプリケーション プロトコル（DNS、SSH など）を検査します。クライアント アプリケーション（PuTTY や Firefox など）や Web アプリケーション（Facebook や Pandora など）を特に検査するように [アプリケーション情報（Application Information）] セクションを設定することもできます。

[アプリケーション情報（Application Information）] セクションのグラフとリストの詳細については、次のトピックを参照してください。

- [リスク/ビジネスとの関連性およびアプリケーション別のトラフィック（Traffic by Risk/Business Relevance and Application）] グラフの表示（56-14 ページ）
- [リスク/ビジネスとの関連性およびアプリケーション別の侵入イベント（Intrusion Events by Risk/Business Relevance and Application）] グラフの表示（56-15 ページ）
- [リスク/ビジネスとの関連性およびアプリケーション別のホスト（Hosts by Risk/Business Relevance and Application）] グラフの表示（56-16 ページ）
- [アプリケーション詳細リスト（Application Details List）] の表示（56-16 ページ）

[アプリケーション情報（Application Information）] セクションのフォーカスを設定するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [Context Explorer] を選択します。

Context Explorer が表示されます。

手順 2　[アプリケーション プロトコル情報（Application Protocol Information）] セクションにポインタを置きます。（同じ Context Explorer セッションで以前にこの設定を変更している場合は、セクション タイトルが [クライアント アプリケーション情報（Client Application Information）] または [Web アプリケーション情報（Web Application Information）] と表示されることがある点に注意してください）。

セクションのオプション ボタンが右上に表示されます。

手順 3　[アプリケーション プロトコル（Application Protocol）]、[クライアント アプリケーション（Client Application）]、または [Web アプリケーション（Web Application）] をクリックします。

[アプリケーション情報（Application Information）] セクションは、選択したオプションに従って更新されます。

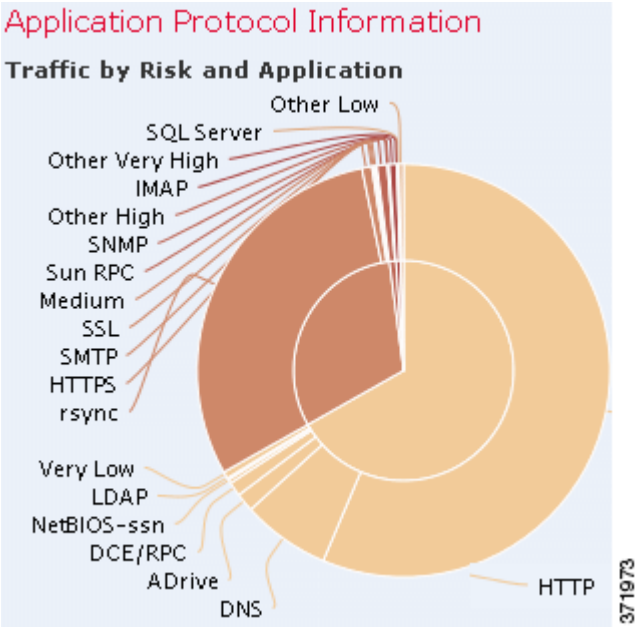
（注）　Context Explorer の外部に移動すると、このセクションはデフォルトの状態（Application Protocol）に戻ります。

[リスク/ビジネスとの関連性およびアプリケーション別のトラフィック(Traffic by Risk/Business Relevance and Application)] グラフの表示

ライセンス:FireSIGHT

[リスク/ビジネスとの関連性およびアプリケーション別のトラフィック(Traffic by Risk/Business Relevance and Application)] グラフはドーナツ形式であり、モニタ対象ネットワークで検出されたアプリケーション トラフィックを、アプリケーションの推定のリスク(デフォルト)または推定のビジネスとの関連性ごとの割合で表示します。内側のリングは推定のリスク/ビジネスとの関連性レベル(Medium または High など)ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション(SSH または NetBIOS など)ごとに分割されます。稀に検出されるアプリケーションは [その他(Other)] にまとめられます。

このグラフは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Explorer の時間範囲を変更しても、グラフは変化しません。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、ビジネスとの関連性とアプリケーションごとにトラフィックが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Business Relevance] をクリックします。デフォルト ビューに戻すには [リスク(Risk)] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトの [リスク(Risk)] ビューに戻ることに注意してください。

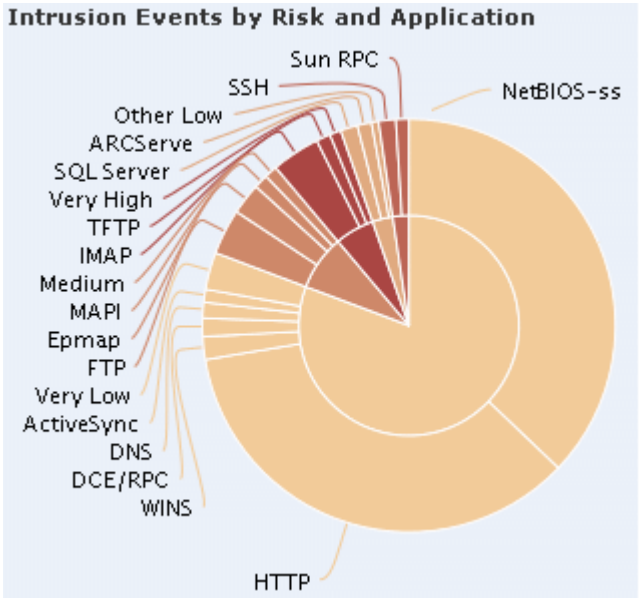
(注)　侵入イベントの情報でフィルタリングすると、[リスク/ビジネスおよびアプリケーション別のトラフィック(Traffic by Risk/Business and Application)] グラフは非表示になります。

このグラフのデータは主に [接続イベント(Connection Events)] 表と [アプリケーション統計(Application Statistics)] 表から取得されます。

[リスク/ビジネスとの関連性およびアプリケーション別の侵入イベント(Intrusion Events by Risk/Business Relevance and Application)] グラフの表示

ライセンス:FireSIGHT

[リスク/ビジネスとの関連性およびアプリケーション別の侵入イベント(Intrusion Events by Risk/Business Relevance and Application)] グラフはドーナツ形式であり、モニタ対象ネットワークで検出された侵入イベントと、これらのイベントに関連するアプリケーションを、アプリケーションの推定のリスク(デフォルト)または推定のビジネスとの関連性ごとの割合で表示します。内側のリングは推定のリスク/ビジネスとの関連性レベル(`Medium` または `High` など)ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション(`SSH` または `NetBIOS` など)ごとに分割されます。稀に検出されるアプリケーションは [その他(Other)] にまとめられます。



ドーナツ グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされるか、または(該当する場合には)アプリケーション情報が表示されます。

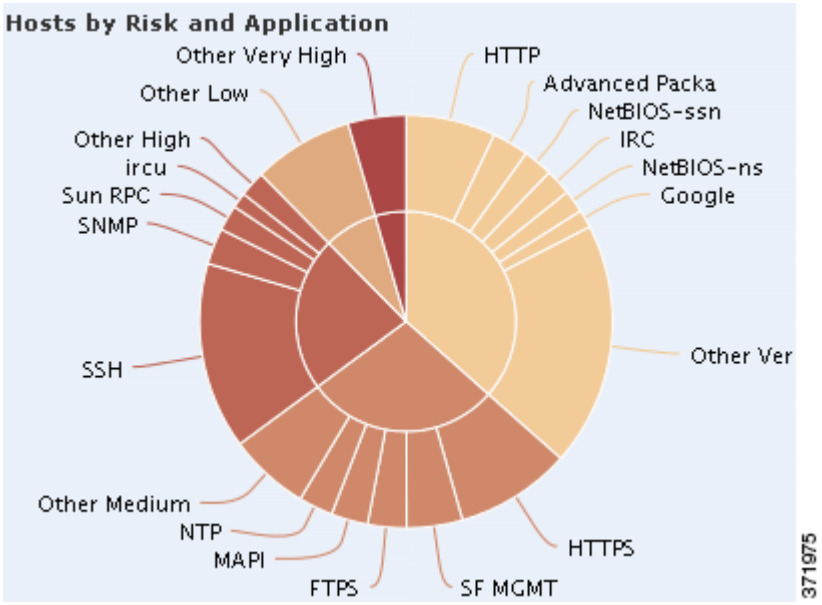
ヒント　グラフに制約を適用して、ビジネスとの関連性とアプリケーションごとに侵入イベントが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [ビジネスとの関連性(Business Relevance)] をクリックします。デフォルト ビューに戻すには [リスク(Risk)] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトの [リスク(Risk)] ビューに戻ることに注意してください。

このグラフのデータは主に [侵入イベント(Intrusion Events)] 表と [アプリケーション統計(Application Statistics)] 表から取得されます。

[リスク/ビジネスとの関連性およびアプリケーション別のホスト(Hosts by Risk/Business Relevance and Application)] グラフの表示

ライセンス: FireSIGHT

[リスク/ビジネスとの関連性およびアプリケーション別のホスト(Hosts by Risk/Business Relevance and Application)] グラフはドーナツ形式であり、モニタ対象ネットワークで検出されたホストと、これらのホストに関連するアプリケーションを、アプリケーションの推定のリスク(デフォルト)または推定のビジネスとの関連性ごとの割合で表示します。内側のリングは推定のリスク/ビジネスとの関連性レベル(`Medium` または `High` など)ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション(`SSH` または `NetBIOS` など)ごとに分割されます。非常に少数のアプリケーションは [その他(Other)] にまとめられます。



ドーナツ グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、ビジネスとの関連性とアプリケーションに基づいてホストが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [ビジネスとの関連性(Business Relevance)] をクリックします。デフォルト ビューに戻すには [リスク(Risk)] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトの [リスク(Risk)] ビューに戻ることに注意してください。

このグラフのデータは主に [アプリケーション(Applications)] 表から取得されます。

[アプリケーション詳細リスト(Application Details List)] の表示

ライセンス: FireSIGHT

[アプリケーション情報(Application Information)] セクション下部に表示される [アプリケーション詳細リスト(Application Details List)] は、モニタ対象ネットワークで検出される各アプリケーションの推定のリスク、推定のビジネスとの関連性、カテゴリ、およびホスト数の情報を示す表です。アプリケーションは、関連ホスト数の降順でリストされます。

[アプリケーション詳細リスト（Application Details List）] 表はソートできませんが、表の項目をクリックして、その情報でフィルタリングまたはドリルダウンしたり、（該当する場合に）アプリケーション情報を表示したりすることができます。この表のデータは主に [アプリケーション（Applications）] 表から取得されます。

このリストは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Explorer の時間範囲を変更しても、リストは変化しません。

[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

ライセンス：Protection

サポートされるデバイス：すべて（シリーズ 2 を除く）

サポートされる防御センター：DC500 を除くいずれか

Context Explorer の [セキュリティ インテリジェンス（Security Intelligence）] セクションには、3 つのインタラクティブな棒グラフが表示されます。これらのグラフは、モニタ対象ネットワーク上でブラックリストに登録されているトラフィックまたは セキュリティ インテリジェンス によってモニタされるトラフィックの概要を示します。これらのグラフでは、カテゴリ、送信元 IP アドレス、および宛先 IP アドレスに基づいてトラフィックがソートされ、トラフィックの容量（KB/秒）と該当する接続の数の両方が表示されます。

[セキュリティ インテリジェンス（Security Intelligence）] セクションのグラフの詳細については、次のトピックを参照してください。

- [カテゴリ別のセキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Category）] グラフの表示（56-17 ページ）
- [送信元 IP 別のセキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Source IP）] グラフの表示（56-18 ページ）
- [宛先 IP 別のセキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Destination IP）] グラフの表示（56-19 ページ）

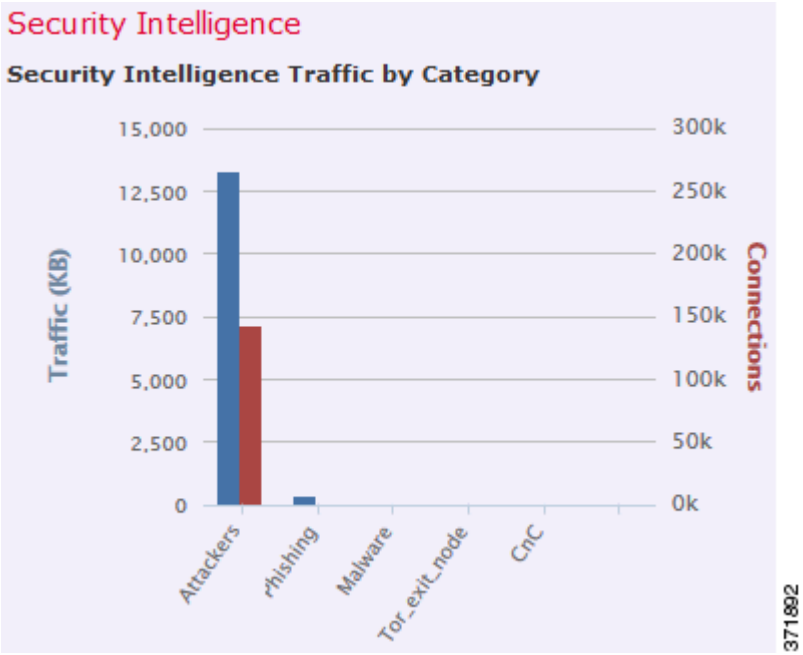
[カテゴリ別のセキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Category）] グラフの表示

ライセンス：Protection

サポートされるデバイス：すべて（シリーズ 2 を除く）

サポートされる防御センター：DC500 を除くいずれか

[カテゴリ別のセキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Category）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上のトラフィックの上位 セキュリティ インテリジェンス カテゴリのネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

(注)　侵入イベントの情報でフィルタリングすると、[カテゴリ別のセキュリティ インテリジェンス トラフィック(Security Intelligence Traffic by Category)] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント(Security Intelligence Events)] 表から取得されます。

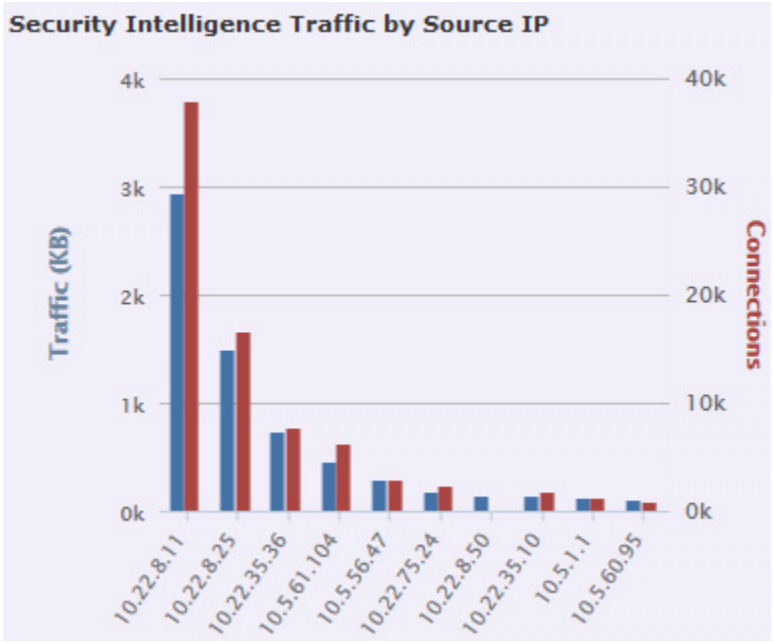
[送信元 IP 別のセキュリティ インテリジェンス トラフィック(Security Intelligence Traffic by Source IP)] グラフの表示

ライセンス: Protection

サポートされるデバイス:すべて(シリーズ 2 を除く)

サポートされる防御センター:DC500 を除くいずれか

[送信元 IP 別のセキュリティ インテリジェンス トラフィック(Security Intelligence Traffic by Source IP)] グラフは棒グラフ形式であり、モニタ対象ネットワーク上のセキュリティ インテリジェンスによってモニタされるトラフィックの上位の送信元 IP アドレスのネットワーク トラフィック カウント(KB/秒)および固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

(注)　侵入イベントの情報でフィルタリングすると、[送信元 IP 別のセキュリティ インテリジェンス トラフィック(Security Intelligence Traffic by Source IP)] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント(Security Intelligence Events)] 表から取得されます。

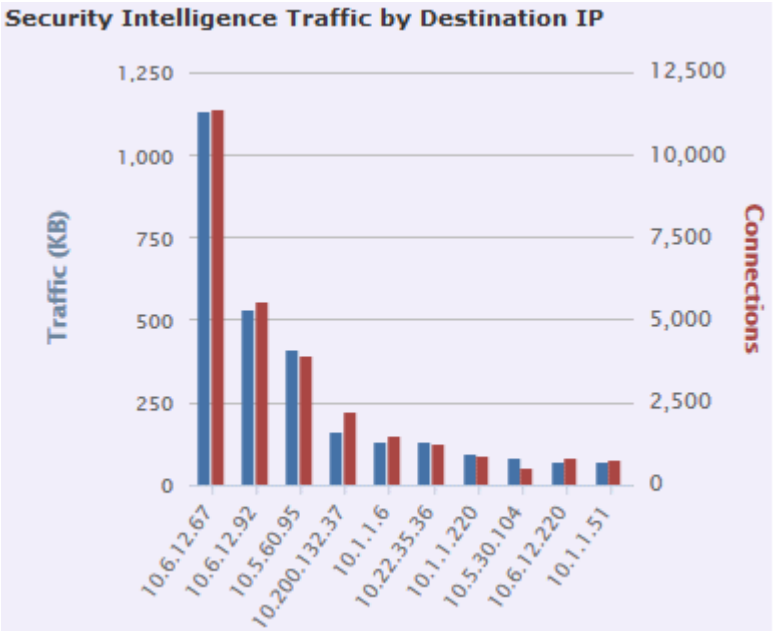
[宛先 IP 別のセキュリティ インテリジェンス トラフィック(Security Intelligence Traffic by Destination IP)] グラフの表示

ライセンス: Protection

サポートされるデバイス:すべて(シリーズ 2 を除く)

サポートされる防御センター:DC500 を除くいずれか

[宛先 IP 別のセキュリティ インテリジェンス トラフィック(Security Intelligence Traffic by Destination IP)] グラフは棒グラフ形式であり、モニタ対象ネットワーク上のセキュリティ インテリジェンスによってモニタされるトラフィックの上位の宛先 IP アドレスのネットワーク トラフィック カウント(KB/秒)および固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

(注)　侵入イベントの情報でフィルタリングすると、[宛先 IP 別のセキュリティ インテリジェンス トラフィック(Security Intelligence Traffic by Destination IP)] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント(Security Intelligence Events)] 表から取得されます。

[侵入情報(Intrusion Information)] セクションについて

ライセンス: Protection

Context Explorer の [侵入情報(Intrusion Information)] セクションには 6 つのインタラクティブ グラフと 1 つの表形式リストが表示されます。これらのグラフとリストは、モニタ対象ネットワークの侵入イベントの概要(侵入イベントに関連付けられている影響レベル、攻撃元、攻撃対象先、ユーザ、優先レベル、およびセキュリティ ゾーンと、侵入イベントの分類、優先度、カウントを示す詳細なリスト)を示します。

[ネットワーク情報(Network Information)] セクションのグラフとリストの詳細については、次のトピックを参照してください。

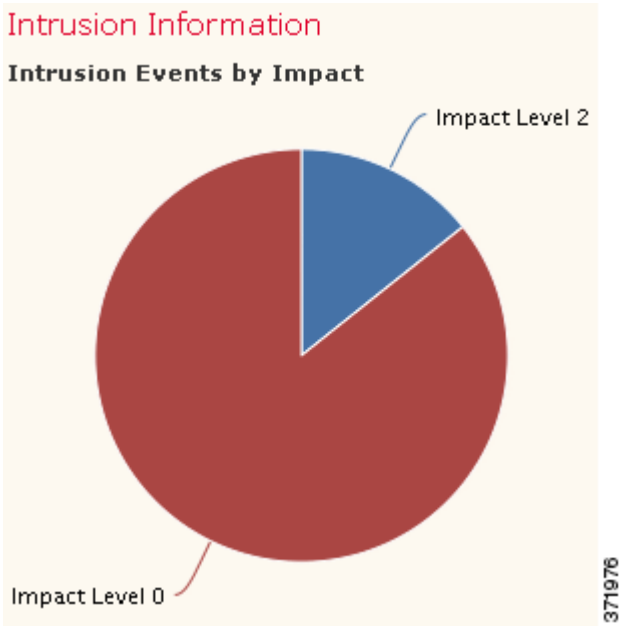
- [影響別の侵入イベント(Intrusion Events by Impact)] グラフの表示(56-21 ページ)
- [上位攻撃者(Top Attackers)] グラフの表示(56-21 ページ)
- [上位ユーザ(Top Users)] グラフの表示(56-22 ページ)
- [プライオリティ別の侵入イベント(Intrusion Events by Priority)] グラフの表示(56-23 ページ)
- [上位ターゲット(Top Targets)] グラフの表示(56-23 ページ)

- [上位の入力/出力セキュリティ ゾーン（Top Ingress/Egress Security Zones）] グラフの表示（56-24 ページ）
- [侵入イベント詳細リスト（Intrusion Event Details List）] の表示（56-25 ページ）

[影響別の侵入イベント（Intrusion Events by Impact）] グラフの表示

ライセンス：Protection

[影響別の侵入イベント（Intrusion Events by Impact）] グラフは円グラフ形式であり、モニタ対象ネットワークの侵入イベントを、推定影響レベル（0 ～ 4）のグループごとの割合のビューで表示します。



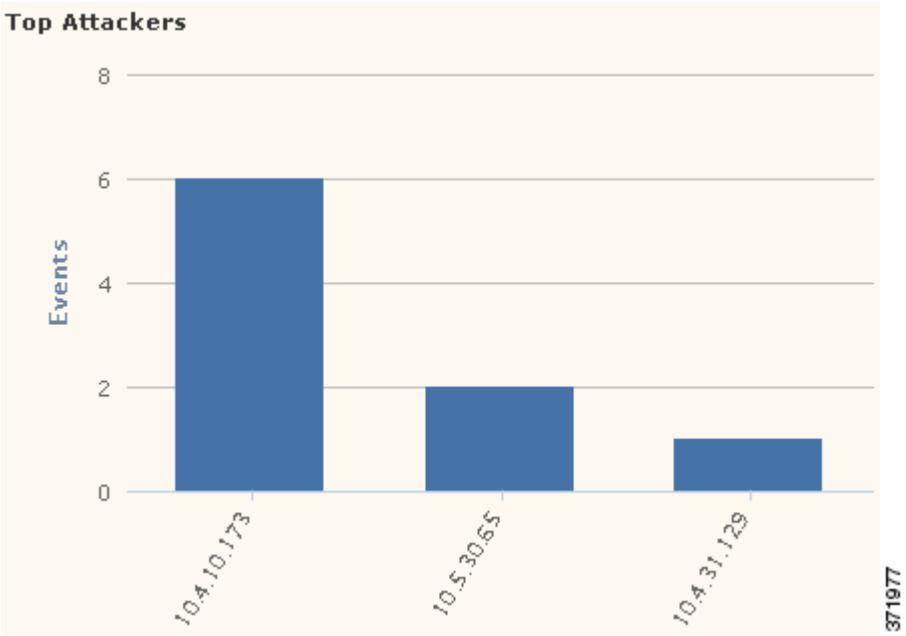
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [侵入イベント（Intrusion Events）] 表と [IDS 統計（IDS Statistics）] 表から取得されます。

[上位攻撃者（Top Attackers）] グラフの表示

ライセンス：Protection

[上位攻撃者（Top Attackers）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の（侵入イベントを発生させた）上位の攻撃元ホスト IP アドレスの侵入イベント数を表示します。



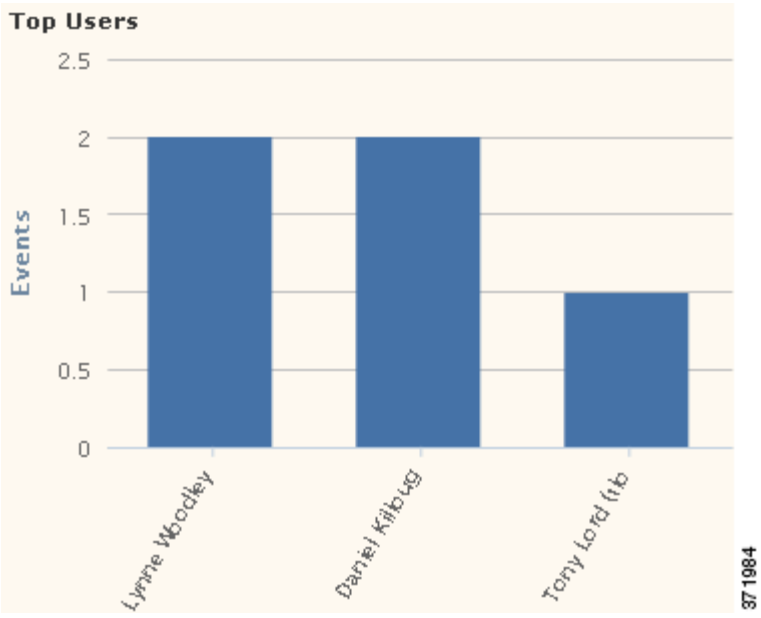
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [侵入イベント（Intrusion Events）] 表から取得されます。

[上位ユーザ（Top Users）] グラフの表示

ライセンス：Protection

[上位ユーザ（Top Users）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最大侵入イベント数に関連するユーザと、イベント数を表示します。



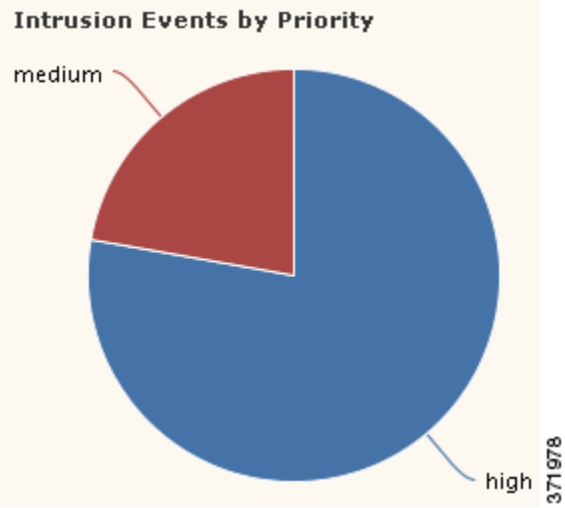
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [侵入イベント（Intrusion Events）] 表と [IDS ユーザ統計（IDS User Statistics）] 表から取得されます。User Agent によって報告されるユーザのみが表示されることに注意してください。

[プライオリティ別の侵入イベント（Intrusion Events by Priority）] グラフの表示

ライセンス：Protection

[プライオリティ別の侵入イベント（Intrusion Events by Priority）] グラフは円グラフ形式であり、モニタ対象ネットワークの侵入イベントを、推定優先度レベル（`High`、`Medium`、`Low` など）のグループごとの割合のビューで表示します。



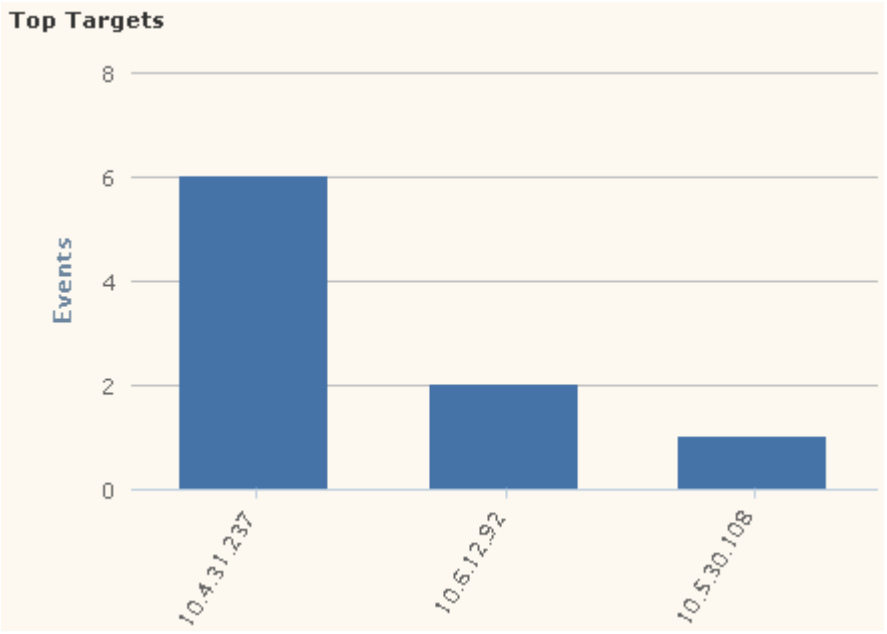
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [侵入イベント（Intrusion Events）] 表から取得されます。

[上位ターゲット（Top Targets）] グラフの表示

ライセンス：Protection

[上位ターゲット（Top Targets）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の（侵入イベントを発生させた接続で攻撃対象となった）上位の攻撃対象ホスト IP アドレスの侵入イベント数を表示します。



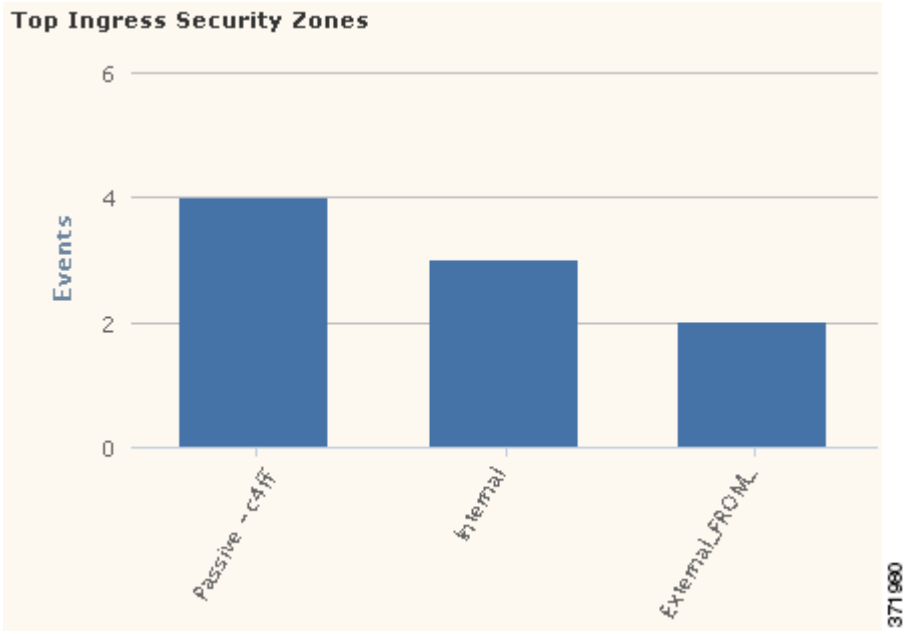
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [侵入イベント（Intrusion Events）] 表から取得されます。

[上位の入力/出力セキュリティ ゾーン（Top Ingress/Egress Security Zones）] グラフの表示

ライセンス：Protection

[上位の入力/出力セキュリティ ゾーン（Top Ingress/Egress Security Zones）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上で設定されている各セキュリティ ゾーン（グラフ設定に応じて入力または出力）に関連する侵入イベントの数を表示します。セキュリティ ゾーンの詳細については、セキュリティ ゾーンの操作（3-44 ページ）を参照してください。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、出力セキュリティ ゾーンのトラフィックのみが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [出力(Egress)] をクリックします。デフォルト ビューに戻すには [入力(Ingress)] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトの [入力(Ingress)] ビューに戻ることに注意してください。

このグラフのデータは主に [侵入イベント(Intrusion Events)] 表から取得されます。

必要に応じて、このグラフに入力(デフォルト)セキュリティ ゾーン情報または出力セキュリティ ゾーン情報のいずれかを表示するように設定できます。

[侵入イベント詳細リスト(Intrusion Event Details List)] の表示

ライセンス: Protection

[侵入情報(Intrusion Information)] セクション下部に表示される [侵入イベント詳細リスト(Intrusion Event Details List)] は、モニタ対象ネットワークで検出される各侵入イベントの分類、推定優先度、およびイベント数の情報を示す表です。イベントは、イベント数の降順でリストされます。

[侵入イベント詳細リスト(Intrusion Event Details List)] 表はソートできませんが、テーブルの項目をクリックして、その情報でフィルタリングまたはドリルダウンすることができます。この表のデータは主に [侵入イベント(Intrusion Events)] 表から取得されます。

[ファイル情報(Files Information)] セクションについて

ライセンス: Protection または Malware

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

Context Explorer の [ファイル情報(Files Information)] セクションには、6 つのインタラクティブ グラフが表示されます。これらのグラフは、モニタ対象ネットワーク上のファイルとマルウェア イベントの概要を示します。このうち 5 つのグラフには、ネットワーク トラフィックで検出されたファイルのファイル タイプ、ファイル名、マルウェアの性質、およびこれらのファイルを送信(アップロード)および受信(ダウンロード)するホストが表示されます。最後のグラフは、ネットワークで検出されたマルウェア脅威を表示し、FireAMP サブスクリプションがある場合はユーザが FireAMP コネクタをインストールしているエンドポイントで検出されたマルウェア脅威も表示します。

(注)　侵入情報でフィルタリングすると、[ファイル情報(File Information)] セクション全体が非表示になります。

[ファイル情報(File Information)] のグラフにネットワークベースのマルウェア データを組み込むには、Malware ライセンスを所有しており、マルウェア検出を有効にしている必要があることに注意してください。また、DC500 防御センターおよびシリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS は、高度なマルウェア防御をサポートしていないため、DC500 防御センターはこのデータを表示できず、シリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS はこのデータを検出しないことに注意してください。マルウェア防御とファイル制御について(37-2 ページ)を参照してください。

[ファイル情報(Files Information)] セクションのグラフの詳細については、次のトピックを参照してください。

- [上位ファイル タイプ(Top File Types)] グラフの表示(56-26 ページ)
- [上位ファイル名(Top File Names)] グラフの表示(56-27 ページ)
- [性質別ファイル(Files by Disposition)] グラフの表示(56-28 ページ)
- [ファイルを送信する上位ホスト(Top Hosts Sending Files)] グラフの表示(56-29 ページ)
- [ファイルを受信する上位ホスト(Top Hosts Receiving Files)] グラフの表示(56-30 ページ)
- [上位マルウェア検出(Top Malware Detections)] グラフの表示(56-31 ページ)

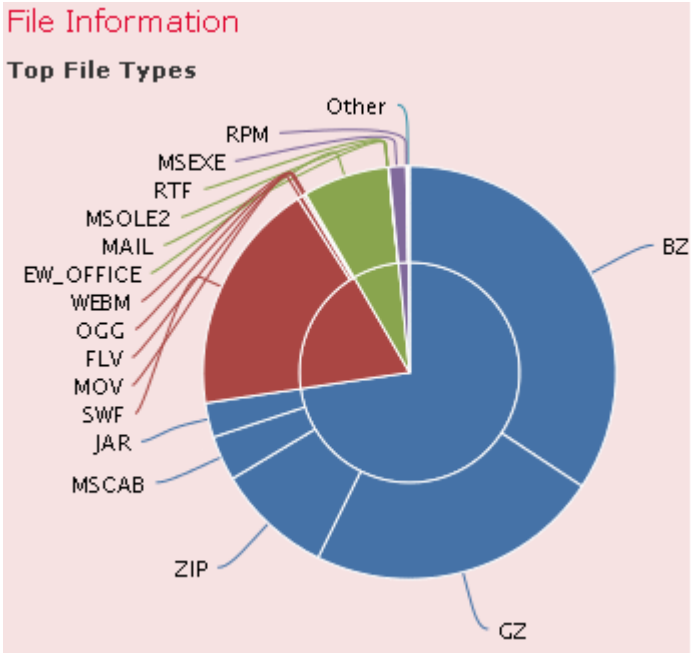
[上位ファイル タイプ(Top File Types)] グラフの表示

ライセンス: Protection または Malware

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

[上位ファイル タイプ(Top File Types)] グラフはドーナツ グラフ形式であり、ネットワーク トラフィックで検出されたファイル タイプ(外部リング)を、ファイル カテゴリ(内部リング)のグループごとの割合のビューで表示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフにネットワークベースのマルウェア データを組み込むには、Malware ライセンスを所有しており、マルウェア検出を有効にしている必要があることに注意してください。また、DC500 防御センターおよびシリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS は、高度なマルウェア防御をサポートしていないため、DC500 防御センターはこのデータを表示できず、シリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS はこのデータを検出しないことに注意してください。マルウェア防御とファイル制御について（37-2 ページ）を参照してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

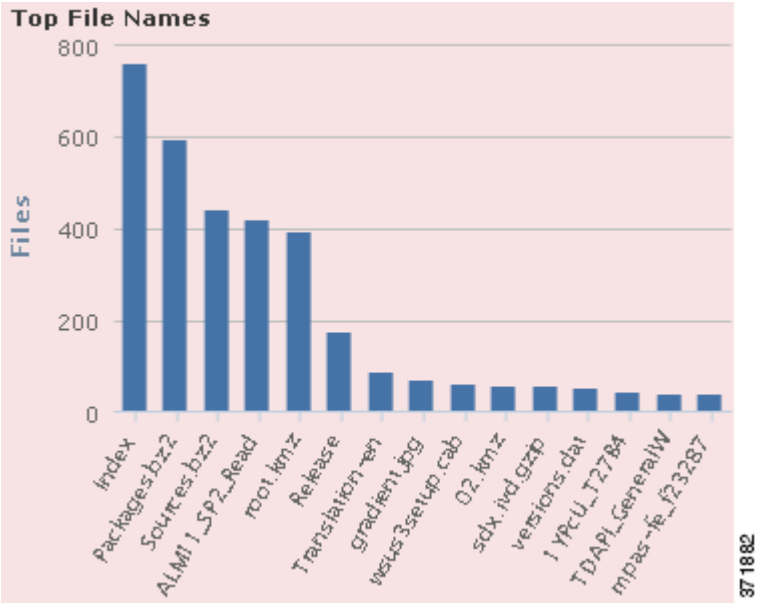
[上位ファイル名（Top File Names）] グラフの表示

ライセンス：Protection または Malware

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

[上位ファイル名（Top File Names）] グラフは棒グラフ形式であり、ネットワーク トラフィックで検出された上位の固有ファイル名の数を表示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフにネットワークベースのマルウェア データを組み込むには、Malware ライセンスを所有しており、マルウェア検出を有効にしている必要があることに注意してください。また、DC500 防御センターおよびシリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS は、高度なマルウェア防御をサポートしていないため、DC500 防御センターはこのデータを表示できず、シリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS はこのデータを検出しないことに注意してください。マルウェア防御とファイル制御について（37-2 ページ）を参照してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

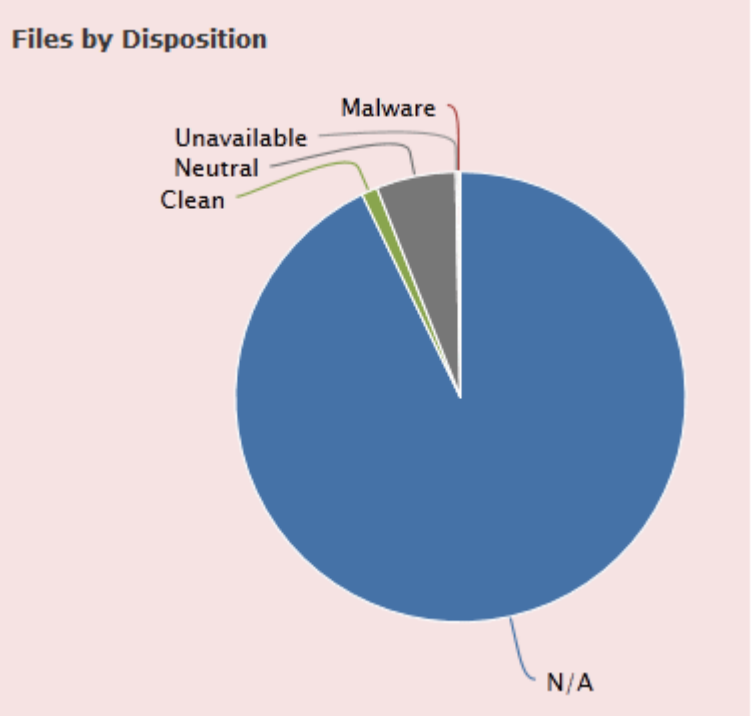
[性質別ファイル（Files by Disposition）] グラフの表示

ライセンス：Protection または Malware

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

[性質別ファイル（Files by Disposition）] グラフは円グラフ形式であり、ネットワーク トラフィックで検出されたファイルのマルウェアの性質の割合のビューを表示します。防御センターが Collective Security Intelligence クラウドルックアップ（Malware ライセンスが必要）を実行したファイルのみが性質を持つことに注意してください。クラウド ルックアップをトリガーしなかったファイルには、`N/A` という性質が設定されます。`Unavailable` という性質は、防御センターがマルウェア クラウド ルックアップを実行できなかったことを示します。他の性質の説明については、マルウェア防御とファイル制御について（37-2 ページ）を参照してください。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフにネットワークベースのマルウェア データを組み込むには、Malware ライセンスを所有しており、マルウェア検出を有効にしている必要があることに注意してください。また、DC500 防御センターおよびシリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS は、高度なマルウェア防御をサポートしていないため、DC500 防御センターはこのデータを表示できず、シリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS はこのデータを検出しないことに注意してください。マルウェア防御とファイル制御について（37-2 ページ）を参照してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

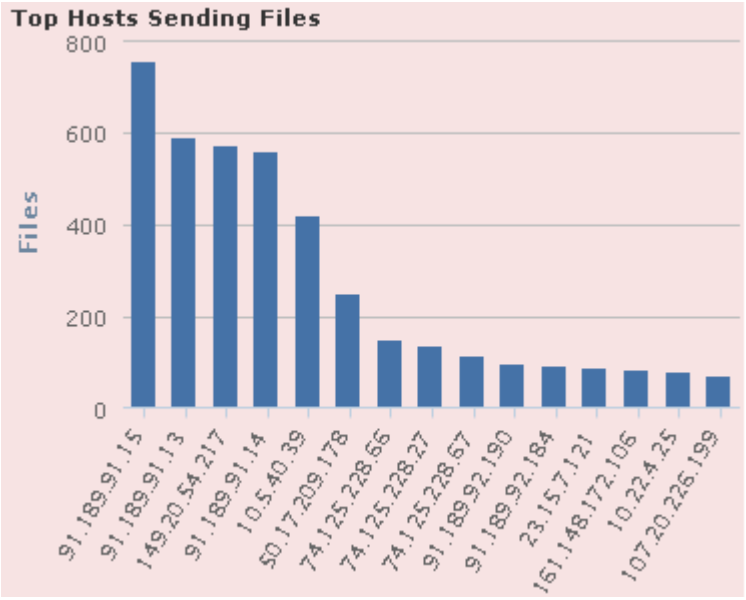
[ファイルを送信する上位ホスト（Top Hosts Sending Files）] グラフの表示

ライセンス：Protection または Malware

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

[ファイルを送信する上位ホスト（Top Hosts Sending Files）] グラフは棒グラフ形式であり、ネットワーク トラフィックで検出された、上位のファイル送信ホスト IP アドレスに対するファイルの数を表示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、マルウェアを送信するホストだけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [マルウェア（Malware）] をクリックします。デフォルトのファイルのビューに戻すには [ファイル（Files）] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトのファイルのビューに戻ることに注意してください。

このグラフにネットワークベースのマルウェア データを組み込むには、Malware ライセンスを所有しており、マルウェア検出を有効にしている必要があることに注意してください。また、DC500 防御センターおよびシリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS は、高度なマルウェア防御をサポートしていないため、DC500 防御センターはこのデータを表示できず、シリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS はこのデータを検出しないことに注意してください。マルウェア防御とファイル制御について（37-2 ページ）を参照してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

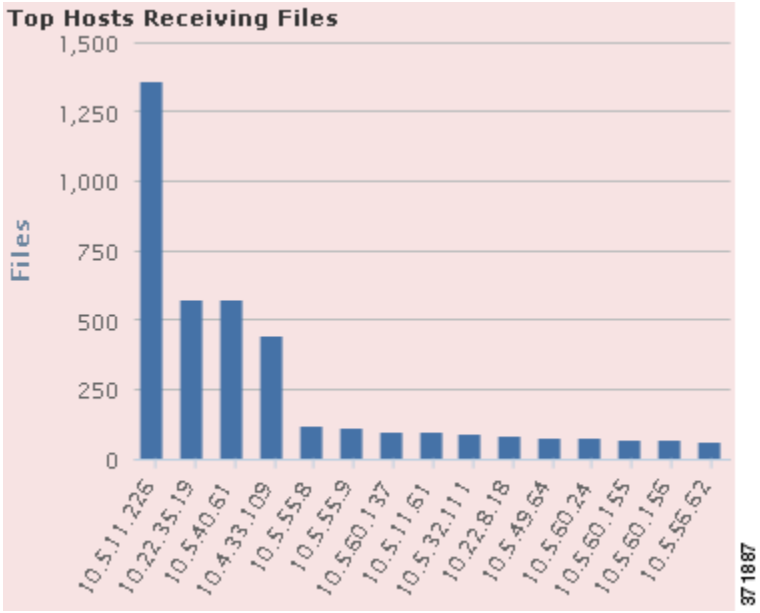
[ファイルを受信する上位ホスト（Top Hosts Receiving Files）] グラフの表示

ライセンス：Protection または Malware

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

[ファイルを受信する上位ホスト（Top Hosts Receiving Files）] グラフは棒グラフ形式であり、ネットワーク トラフィックで検出された、上位のファイル受信ホスト IP アドレスに対するファイルの数を表示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント

グラフに制約を適用して、マルウェアを受信するホストだけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [マルウェア（Malware）] をクリックします。デフォルトのファイルのビューに戻すには [ファイル（Files）] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトのファイルのビューに戻ることに注意してください。

このグラフにネットワークベースのマルウェア データを組み込むには、Malware ライセンスを所有しており、マルウェア検出を有効にしている必要があることに注意してください。また、DC500 防御センターおよびシリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS は、高度なマルウェア防御をサポートしていないため、DC500 防御センターはこのデータを表示できず、シリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS はこのデータを検出しないことに注意してください。マルウェア防御とファイル制御について（37-2 ページ）を参照してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

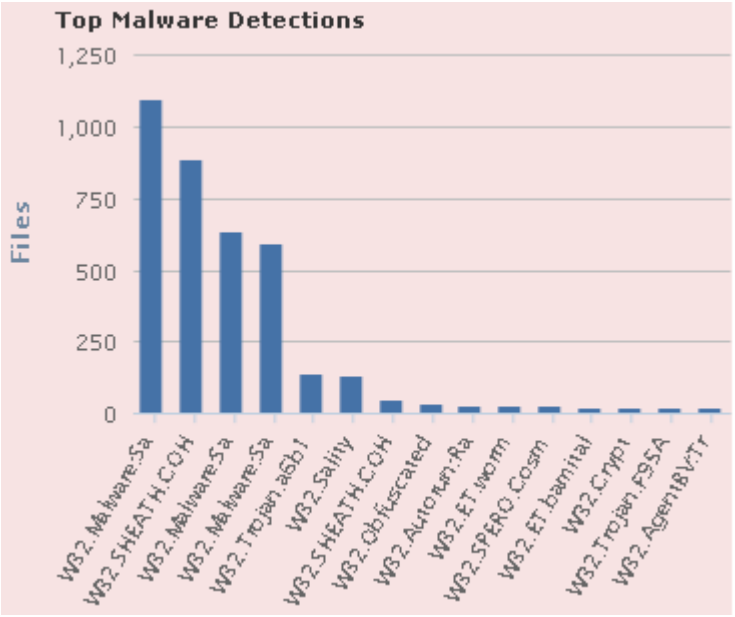
[上位マルウェア検出（Top Malware Detections）] グラフの表示

ライセンス：Protection または Malware

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

[上位マルウェア検出（Top Malware Detections）] グラフは棒グラフ形式であり、ネットワークで検出された上位のマルウェア脅威の数を表示します。また、FireAMP サブスクリプションがある場合は、ユーザが FireAMP コネクタをインストールしているエンドポイントで検出された上位のマルウェア脅威の数も表示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフにネットワークベースのマルウェア データを組み込むには、Malware ライセンスを所有しており、マルウェア検出を有効にしている必要があることに注意してください。また、DC500 防御センターおよびシリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS は、高度なマルウェア防御をサポートしていないため、DC500 防御センターはこのデータを表示できず、シリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS はこのデータを検出しないことに注意してください。マルウェア防御とファイル制御について（37-2 ページ）を参照してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表と [マルウェア イベント（Malware Events）] 表から取得されます。

[地理位置情報（Geolocation Information）] セクションについて

ライセンス：FireSIGHT

サポートされる防御センター：DC500 を除くいずれか

Context Explorer の [地理位置情報（Geolocation Information）] セクションには、3 つのインタラクティブなドーナツ グラフが表示されます。これらのグラフは、モニタ対象ネットワークのホストがデータを交換している国の概要（イニシエータ国またはレスポンダ国ごとの固有接続数、送信元または宛先の国ごとの侵入イベント数、および送信側または受信側の国ごとのファイル イベント数）を示します。

[地理位置情報（Geolocation Information）] セクションのグラフの詳細については、次のトピックを参照してください。

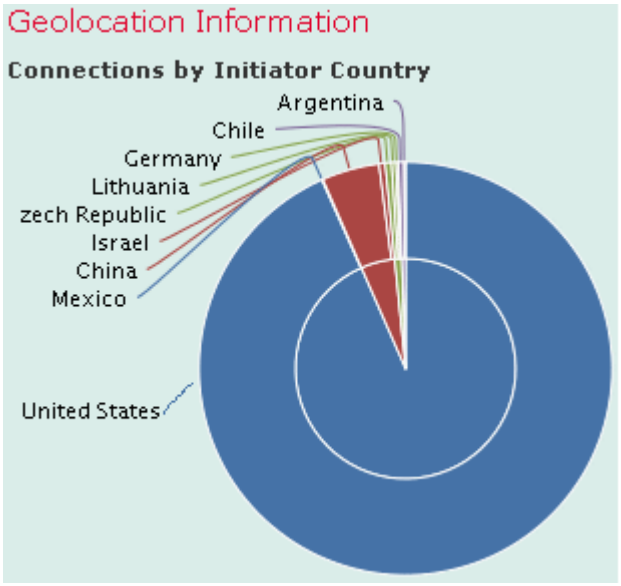
- [イニシエータ/レスポンダ国別の接続（Connections by Initiator/Responder Country）] グラフの表示（56-33 ページ）
- [送信元/宛先国別の侵入イベント（Intrusion Events by Source/Destination Country）] グラフの表示（56-34 ページ）
- [送信/受信国別のファイル イベント（File Events by Sending/Receiving Country）] グラフの表示（56-35 ページ）

[イニシエータ/レスポンダ国別の接続(Connections by Initiator/Responder Country)] グラフの表示

ライセンス: FireSIGHT

サポートされる防御センター:DC500 を除くいずれか

[イニシエータ/レスポンダ国別の接続(Connections by Initiator/Responder Country)] グラフはドーナツ グラフ形式であり、ネットワーク上での接続にイニシエータ(デフォルト)またはレスポンダとして関わる国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。位置情報については、地理位置情報の使用(58-24 ページ)を参照してください。接続データについては、接続およびセキュリティ インテリジェンスのデータの使用(39-1 ページ)を参照してください。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、接続でレスポンダとなっている国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [レスポンダ(Responder)] をクリックします。デフォルト ビューに戻すには [イニシエータ(Initiator)] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトの [イニシエータ(Initiator)] ビューに戻ることに注意してください。

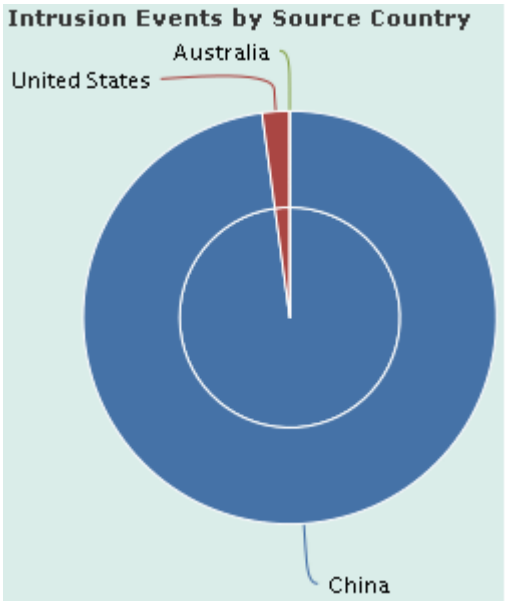
このグラフのデータは主に [サマリ データ別の接続(Connection Summary Data)] 表から取得されます。

[送信元/宛先国別の侵入イベント（Intrusion Events by Source/Destination Country）] グラフの表示

ライセンス：FireSIGHT

サポートされる防御センター：DC500 を除くいずれか

[送信元/宛先国別の侵入イベント（Intrusion Events by Source/Destination Country）] グラフはドーナツ グラフ形式であり、ネットワーク上の侵入イベントにイベントの送信元（デフォルト）または宛先として関わる国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。位置情報については、地理位置情報の使用（58-24 ページ）を参照してください。侵入イベント データについては、侵入イベントの操作（41-1 ページ）を参照してください。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、侵入イベントの宛先となっている国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [宛先（Destination）] をクリックします。デフォルト ビューに戻すには [送信元（Source）] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトの [送信元（Source）] ビューに戻ることに注意してください。

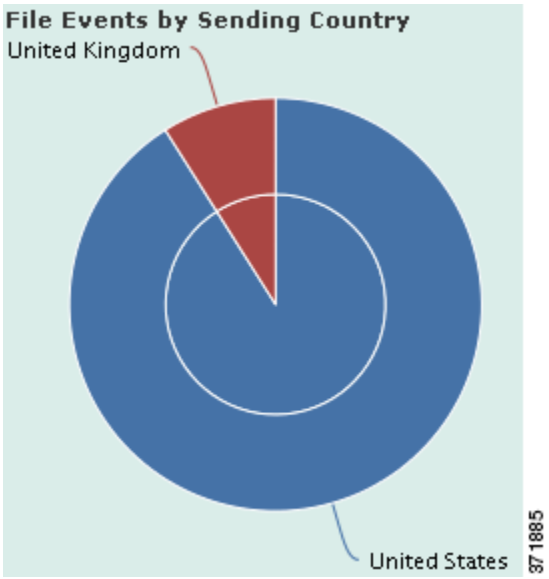
このグラフのデータは主に [侵入イベント（Intrusion Events）] 表から取得されます。

[送信/受信国別のファイル イベント(File Events by Sending/Receiving Country)] グラフの表示

ライセンス: FireSIGHT

サポートされる防御センター:DC500 を除くいずれか

[送信/受信国別のファイル イベント(File Events by Sending/Receiving Country)] グラフはドーナツ グラフ形式であり、ネットワーク上のファイル イベントでファイルの送信側(デフォルト)または受信側として検出された国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。位置情報については、地理位置情報の使用(58-24 ページ)を参照してください。ファイル イベント データについては、ファイル イベントの操作(40-8 ページ)を参照してください。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、ファイルを受信する国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [受信者(Receiver)] をクリックします。デフォルト ビューに戻すには [送信者(Sender)] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトの [送信者(Sender)] ビューに戻ることに注意してください。

このグラフのデータは主に [ファイル イベント(File Events)] 表から取得されます。

[URL 情報（URL Information）] セクションについて

ライセンス：FireSIGHT または URL フィルタリング（URL Filtering）

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

Context Explorer の [URL 情報（URL Information）] セクションには、3 つのインタラクティブ グラフが表示されます。これらのグラフは、モニタ対象ネットワーク上のホストがデータを交換する URL の概要（URL に関連付けられているトラフィックおよび固有接続数を個々の URL、URL カテゴリ、および URL レピュテーションごとにソートしたもの）を示します。URL 情報でフィルタリングすることはできません。

（注）　侵入イベント情報でフィルタリングすると、[URL 情報（URL Information）] セクション全体が非表示になります。

URL フィルタリング グラフに URL カテゴリとレピュテーションのデータを組み込むには、URL フィルタリング（URL Filtering）ライセンスを所有しており、URL フィルタリング（URL Filtering）を有効にしている必要があることに注意してください。また、DC500 防御センターとシリーズ 2 デバイスはいずれも、レピュテーションとカテゴリによる URL フィルタリングをサポートしていないため、DC500 防御センターはこのデータを表示できず、シリーズ 2デバイスはこのデータを検出しないことにも注意してください。URL のブロッキング（16-10 ページ）を参照してください。

[URL 情報（URL Information）] セクションのグラフの詳細については、次のトピックを参照してください。

- [URL 別のトラフィック（Traffic by URL）] グラフの表示（56-36 ページ）
- [URL カテゴリ別のトラフィック（Traffic by URL Category）] グラフの表示（56-37 ページ）
- [URL レピュテーション別のトラフィック（Traffic by URL Reputation）] グラフの表示（56-38 ページ）

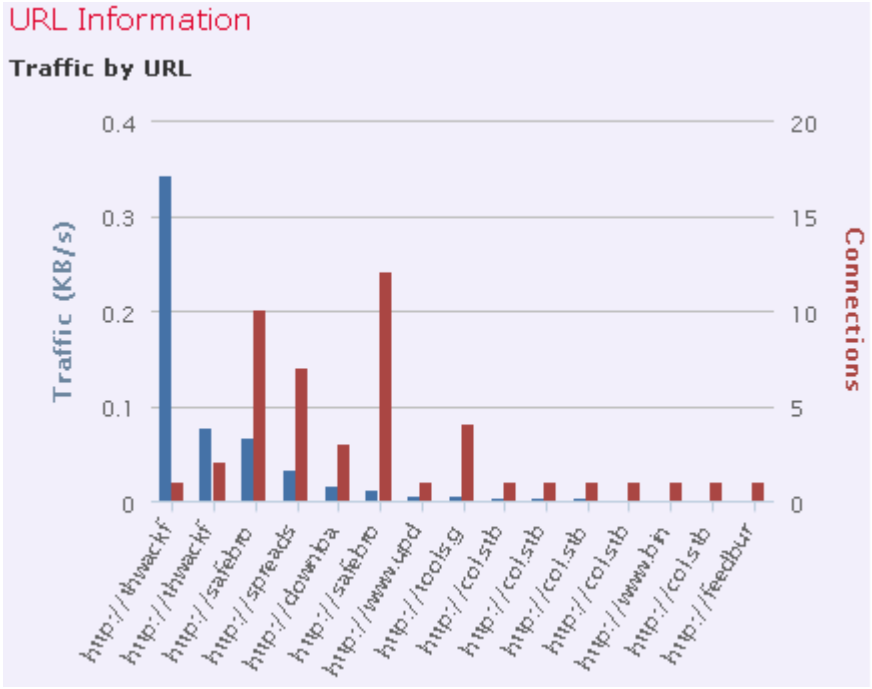
[URL 別のトラフィック（Traffic by URL）] グラフの表示

ライセンス：FireSIGHT または URL フィルタリング（URL Filtering）

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

[URL 別のトラフィック（Traffic by URL）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最も要求される上位 15 の URL のネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされた URL ごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

(注)　侵入イベントの情報でフィルタリングすると、[URL 別のトラフィック(Traffic by URL)] グラフは非表示になります。

URL フィルタリング グラフに URL カテゴリとレピュテーションのデータを組み込むには、URL フィルタリング(URL Filtering)ライセンスを所有しており、URL フィルタリング(URL Filtering)を有効にしている必要があることに注意してください。また、DC500 防御センターとシリーズ 2 デバイスはいずれも、レピュテーションとカテゴリによる URL フィルタリングをサポートしていないため、DC500 防御センターはこのデータを表示できず、シリーズ 2デバイスはこのデータを検出しないことにも注意してください。クラウド通信の有効化(64-30 ページ)を参照してください。

このグラフのデータは主に [接続イベント(Connection Events)] 表から取得されます。

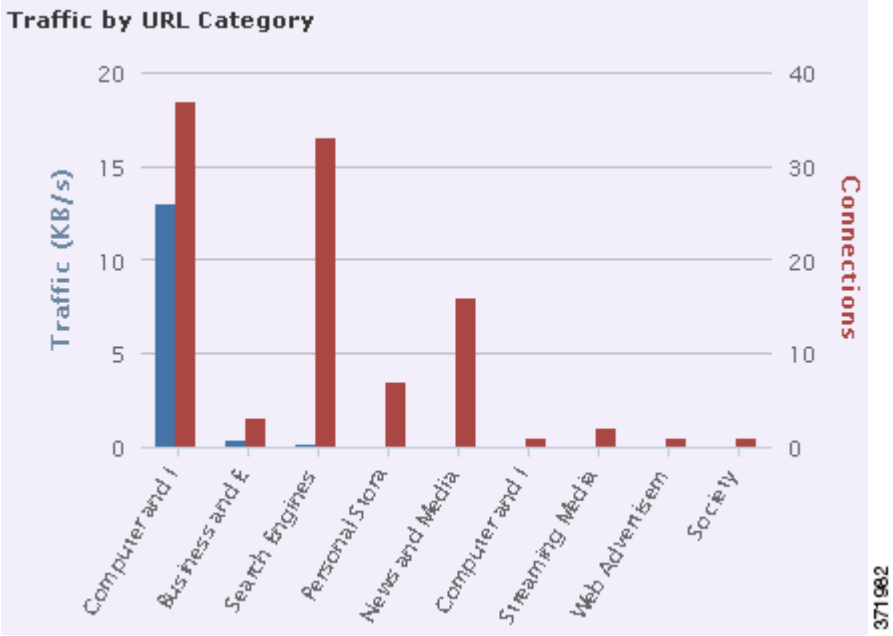
[URL カテゴリ別のトラフィック(Traffic by URL Category)] グラフの表示

ライセンス:URL フィルタリング(URL Filtering)

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

[URL カテゴリ別のトラフィック(Traffic by URL Category)] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最も要求される URL カテゴリ(`Search Engines`、`Streaming Media` など)のネットワーク トラフィック カウント(KB/秒)および固有接続数を表示します。リストされた URL カテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

(注)　侵入イベントの情報でフィルタリングすると、[URL カテゴリ別のトラフィック（Traffic by URL Category）] グラフは非表示になります。

URL フィルタリング グラフに URL カテゴリとレピュテーションのデータを組み込むには、URL フィルタリング（URL Filtering）ライセンスを所有しており、URL フィルタリング（URL Filtering）を有効にしている必要があることに注意してください。また、DC500 防御センターとシリーズ 2 デバイスはいずれも、レピュテーションとカテゴリによる URL フィルタリングをサポートしていないため、DC500 防御センターはこのデータを表示できず、シリーズ 2デバイスはこのデータを検出しないことにも注意してください。レピュテーション ベースの URL ブロッキングの実行（16-12 ページ）を参照してください。

このグラフのデータは主に [URL 統計（URL Statistics）] 表と [接続イベント（Connection Events）] 表から取得されます。

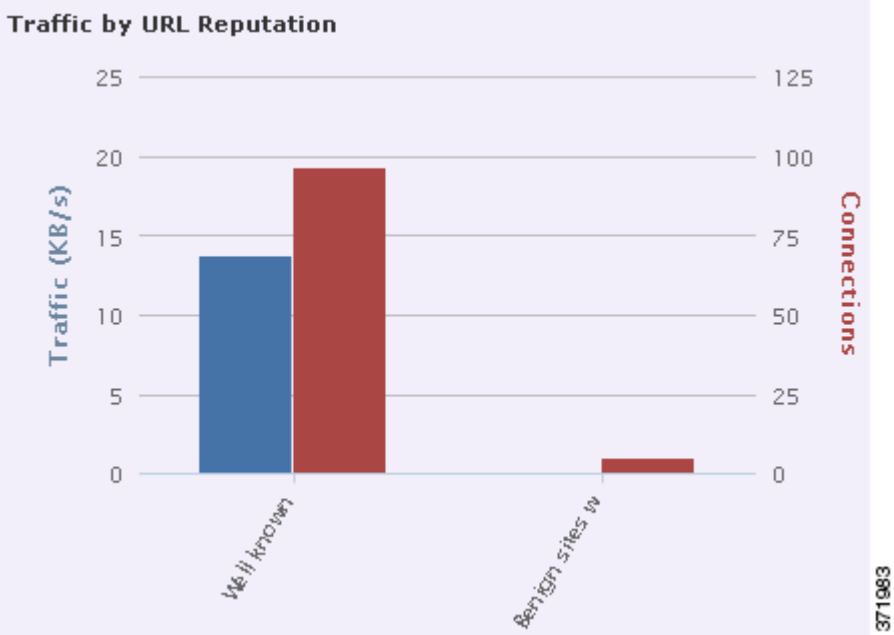
[URL レピュテーション別のトラフィック（Traffic by URL Reputation）] グラフの表示

ライセンス：URL フィルタリング（URL Filtering）

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

[URL レピュテーション別のトラフィック（Traffic by URL Reputation）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最も要求される URL レピュテーション グループ（`Well known`、`Benign sites with security risks` など）のネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされた URL レピュテーションごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。



グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

(注)　侵入イベントの情報でフィルタリングすると、[URL レピュテーション別のトラフィック（Traffic by URL Reputation）] グラフは非表示になります。

URL フィルタリング グラフに URL カテゴリとレピュテーションのデータを組み込むには、URL フィルタリング（URL Filtering）ライセンスを所有しており、URL フィルタリング（URL Filtering）を有効にしている必要があることに注意してください。また、DC500 防御センターとシリーズ 2 デバイスはいずれも、レピュテーションとカテゴリによる URL フィルタリングをサポートしていないため、DC500 防御センターはこのデータを表示できず、シリーズ 2デバイスはこのデータを検出しないことにも注意してください。レピュテーション ベースの URL ブロッキングの実行（16-12 ページ）を参照してください。

このグラフのデータは主に [URL 統計（URL Statistics）] 表と [接続イベント（Connection Events）] 表から取得されます。

Context Explorer の更新

ライセンス：FireSIGHT

Context Explorer は、表示情報を自動的に更新しません。新しいデータを組み込むには、Explorer を手動で更新する必要があります。

Context Explorer 自体をリロードすると（ブラウザ プログラムの更新または Context Explorer から外部へ移動した後に戻る操作など）、すべての表示情報が更新されますが、セクション設定（Ingress/Egress グラフや [アプリケーション情報（Application Information）] セクションなど）に対して行った変更は保持されず、また、読み込みに時間がかかることがある点に注意してください。

Context Explorer の更新方法:

アクセス: Admin/Any Security Analyst

手順 1　Context Explorer の右上にある [リロード(Reload)] をクリックします。

Explorer が更新され、選択した時間範囲内の最新情報が表示されます。更新が完了するまでは [リロード(Reload)] ボタンがグレー表示になることに注意してください。

Context Explorer の時間範囲の設定

ライセンス: FireSIGHT

過去 1 時間(デフォルト)から過去 1 年までの期間を反映するように、Context Explorer の時間範囲を設定できます。時間範囲を変更しても、Context Explorer は自動的に変更を反映する更新をしないことに注意してください。新しい時間範囲を適用するには、Explorer を手動で更新する必要があります。

時間範囲の変更は、Context Explorer から外部に移動したり、ログイン セッションを終了したりしても維持されます。

Context Explorer の時間範囲を変更するには、次の手順を実行します。

アクセス: Admin/Any Security Analyst

手順 1　[最新を表示(Show the last)] ドロップダウンリストから時間範囲を選択します。

手順 2　オプションで、新しい時間範囲のデータを表示するには、[リロード(Reload)] をクリックします。

Context Explorer のすべてのセクションが更新され、新しい時間範囲が反映されます。

ヒント　[フィルタの適用(Apply Filters)] をクリックすると、時間範囲の更新が適用されます。

Context Explorer のセクションの最小化および最大化

ライセンス: FireSIGHT

Context Explorer では 1 つ以上のセクションを最小化して非表示にできます。これは、特定のセクションだけを強調する場合や、ビューをシンプルにしたい場合に便利です。[トラフィックおよび侵入イベント カウント タイム(Traffic and Intrusion Event Counts Time)] グラフは最小化できません。

Context Explorer のセクションでは、ページを更新したり、アプライアンスからログアウトしたりしても、設定した最小化または最大化の状態が維持されることに注意してください。

Context Explorer のセクションを最小化する方法:

アクセス: Admin/Any Security Analyst

手順 1　セクションのタイトル バーの最小化アイコン(−)をクリックします。

Context Explorer のセクションを最大化する方法:

アクセス: Admin/Any Security Analyst

手順 1　最小化されているセクションのタイトル バーの最大化アイコン(□)をクリックします。

Context Explorer データのドリルダウン

ライセンス: 機能に応じて異なる

Context Explorer で許容されている詳細レベルよりもさらに詳細にグラフを調べたりデータをリストしたりするには、当該データのテーブル ビューにドリルダウンします。([経時トラフィックおよび侵入イベント(Traffic and Intrusion Events over Time)] グラフではドリル ダウンできないことに注意してください。)たとえば、[送信元 IP 別トラフィック(Traffic by Source IP)] グラフの IP アドレスでドリルダウンすると、[接続イベント(Connection Events)] 表の [アプリケーション詳細で接続(Connections with Application Details)] ビューが表示されます。このビューには、選択した送信元 IP アドレスに関連するデータのみが表示されます。

調べるデータのタイプに応じて、コンテキスト メニューに追加のオプションが表示されることがあります。特定の IP アドレスに関連付けられているデータ ポイントの場合、選択した IP アドレスのホストまたは whois 情報を表示するためのオプションが表示されます。特定のアプリケーションに関連付けられているデータ ポイントの場合、選択したアプリケーションに関するアプリケーション情報を表示するためのオプションが表示されます。特定のユーザに関連付けられているデータ ポイントの場合、ユーザのユーザ プロファイル ページを表示するためのオプションが表示されます。侵入イベントのメッセージに関連付けられているデータ ポイントの場合、そのイベントに関連する侵入ルールに関するルール ドキュメントを表示するオプションが表示されます。特定の IP アドレスに関連付けられているデータ ポイントの場合、そのアドレスをブラックリストまたはホワイトリストに追加するためのオプションが表示されます。

データのドリルダウンに使用するコンテキスト メニューには、そのデータをフィルタリングするためのオプションも含まれています。フィルタリングの詳細については、Context Explorer でのフィルタの操作(56-43 ページ)を参照してください。

Context Explorer でデータをドリルダウンする方法:

アクセス: Admin/Any Security Analyst

手順 1　[分析(Analysis)] > [Context Explorer] を選択します。

Context Explorer が表示されます。

手順 2　[経時トラフィックおよび侵入イベント(Traffic and Intrusion Events over Time)] 以外の任意のセクションで、調査するデータ ポイントをクリックします。

コンテキスト メニュー ポップアップ ウィンドウが表示されます。

手順 3　選択するデータ ポイントに応じて、表示されるオプションが異なります。

- テーブル ビューでこのデータの詳細を表示するには、[分析にドリル（Drill into Analysis）] を選択します。

  新しいウィンドウが開き、選択したデータの詳細なテーブル ビューが表示されます。

- 特定の IP アドレスに関連付けられているデータ ポイントを選択している場合に、関連するホストに関する詳細情報を参照するには、[ホスト情報の表示（View Host Information）] を選択します。

  新しいウィンドウが開き、選択した IP アドレスのホスト プロファイル ページが表示されます。ホスト属性とホスト プロファイルの詳細については、ホスト プロファイルの使用（49-1 ページ）を参照してください。

- 特定の IP アドレスのデータ ポイントを選択している場合に、そのアドレスで whois 検索を行うには、[Whois] を選択します。

  新しいウィンドウが開き、選択した IP アドレスの whois クエリの結果が表示されます。

- 特定のアプリケーションに関連付けられているデータ ポイントを選択している場合に、そのアプリケーションに関する詳細情報を参照するには、[アプリケーション情報の表示（View Application Information）] を選択します。

  新しいウィンドウが開き、選択したアプリケーションの情報が表示されます。アプリケーション属性の詳細については、アプリケーション検出について（45-11 ページ）を参照してください。

- 特定のユーザに関連付けられているデータ ポイントを選択している場合に、そのユーザに関する詳細情報を参照するには、[ユーザ情報の表示（View User Information）] を選択します。

  新しいウィンドウが開き、選択したユーザのユーザ プロファイル ページが表示されます。ユーザ詳細について詳しくは、ユーザの詳細とホストの履歴について（50-68 ページ）を参照してください。

- 特定の侵入イベント メッセージに関連付けられているデータ ポイントを選択している場合に、関連する侵入ルールに関する詳細情報を参照するには、[ルール情報の表示（View Rule Documentation）] を選択します。

  新しいウィンドウが開き、選択したイベントに関連するルール詳細ページが表示されます。侵入ルール詳細について詳しくは、ルール詳細の表示（32-5 ページ）を参照してください。

- 特定の IP アドレスに関連付けられているデータ ポイントを選択している場合に、Security Intelligence グローバル ブラックリストまたはホワイトリストにその IP アドレスを追加するには、[今すぐブラックリストに登録（Blacklist Now）] または [今すぐホワイトリストに登録（Whitelist Now）] のいずれか該当するオプションを選択してください。表示されるポップアップ ウィンドウで選択内容を確認します。

  IP アドレスがブラックリストまたはホワイトリストに登録されます。詳細については、グローバル ホワイトリストおよびブラックリストの操作（3-7 ページ）を参照してください。

  Security Intelligence データをサポートしていない DC500 防御センターでは、これらのオプションは表示されません。

Context Explorer でのフィルタの操作

ライセンス: FireSIGHT

Context Explorer に最初に表示される基本的で広範なデータをフィルタリングして、ネットワーク上のアクティビティの詳細な状況を把握することができます。フィルタは URL 情報以外のすべての種類の FireSIGHT データに対応し、除外と包含がサポートされており、Context Explorer のグラフ データ ポイントをクリックするだけですぐに適用でき、Explorer 全体に反映されます。ネットワークおよび組織のニーズに合った独自の設定にするために、一度に最大 20 個のフィルタを適用できます。適用するフィルタは Context Explorer URL に反映されるため、有用なフィルタ セットはブラウザ プログラムで後で使用できるようにブックマークしておくことができます。

Context Explorer でのフィルタの使用法については、次のトピックを参照してください。

- フィルタの追加および適用（56-43 ページ）
- コンテキスト メニューを使用したフィルタの作成（56-47 ページ）
- フィルタのブックマーク（56-48 ページ）

フィルタの追加および適用

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

Context Explorer データにフィルタを追加する方法はいくつかあります。

- [フィルタの追加（Add Filter）] ウィンドウを使用する。
- コンテキスト メニュー ポップアップ ウィンドウを使用する（Explorer のデータ ポイントを選択する場合）。
- Context Explorer アイコン（ ）または特定の詳細ビュー ページ（[アプリケーション詳細（Application Detail）]、[ホスト プロファイル（Host Profile）]、[ルール詳細（Rule Detail）]、[ユーザ プロファイル（User Profile）]）に表示されるテキスト リンクを使用する。これらのリンクをクリックすると、Context Explorer が自動的に開き、詳細ビュー ページの当該データに基づいて Context Explorer がフィルタリングされます。たとえば、ユーザ `jenkins` のユーザ詳細ページで [Context Explorer] リンクをクリックすると、Explorer にはそのユーザに関連するデータだけが表示されます。

ここでは、[フィルタの追加（Add Filter）] ウィンドウでフィルタを新規に作成する方法について説明します。コンテキスト メニューを使用して Context Explorer のグラフとリスト データからクイック フィルタを作成する方法については、コンテキスト メニューを使用したフィルタの作成（56-47 ページ）を参照してください。

Context Explorer の左上にある [フィルタ（Filters）] の下のプラス アイコン（ ）をクリックすると表示される [フィルタの追加（Add Filter）] ウィンドウには、[データ タイプ（Data Type）] と [フィルタ（Filter）] の 2 つのフィールドだけが表示されます。

[データ タイプ（Data Type）] ドロップダウンリストには、Context Explorer に制約を適用するために使用できる多数の FireSIGHT システムデータ タイプが含まれています。データ タイプの選択後に、そのタイプの固有の値を [フィルタ（Filter）] フィールドに入力します（たとえば、[大陸（Continent）] タイプの場合は値 `Asia` など）。ユーザ支援のため、[フィルタ（Filter）] フィールドでは、選択したデータ タイプのさまざまな値の例がグレー表示で示されます。（フィールドにデータを入力すると、これらは消去されます）。

次の表に、フィルタとして使用できるデータ タイプと、各データ タイプの例と説明を示します。DC500 防御センターでは、サポートされていない機能のデータは表示されず、シリーズ 2デバイスおよび Blue Coat X-Series 向け Cisco NGIPS では、サポートされていない機能のデータは検出されないことに注意してください。シリーズ 2デバイスおよび Blue Coat X-Series 向け Cisco NGIPS の機能の要約については、各デバイス モデルでサポートされるアクセス制御機能の表を参照してください。

表 56-2　フィルタ データ タイプ

タイプ（Type）	値の例	定義（Definition）
アクセス コントロール アクション（Access Control Action）	Allow、Block	トラフィックを許可またはブロックするためにアクセス コントロール ポリシーにより実行されるアクション
アプリケーション カテゴリ（Application Category）	web browser、email	アプリケーションの主要機能の一般的な分類
アプリケーション	Facebook、HTTP	アプリケーションの名前
アプリケーションのリスク（Application Risk）	Very High、Medium	アプリケーションの推定セキュリティ リスク
アプリケーションタグ（Application Tag）	encrypts communications、sends mail	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを使用できます（タグを使用しないことも可能です）。
アプリケーション タイプ（Application Type）	Client、Web Application	アプリケーション タイプ（アプリケーション プロトコル、クライアント、または Web アプリケーション）
ビジネスとの関連性	Very Low、High	（娯楽ではない）ビジネス アクティビティに対するアプリケーションの推定関連度
大陸（Continent）	North America、Asia	モニタ対象ネットワークで検出されたルーティング可能な IP アドレスに関連付けられている大陸
国（Country）	Canada、Japan	モニタ対象ネットワークで検出されたルーティング可能な IP アドレスに関連付けられている国
Device	device1.example.com、192.168.1.3	モニタ対象ネットワーク上のデバイスの名前または IP アドレス
イベント分類（Event Classification）	Potential Corporate Policy Violation、Attempted Denial of Service	侵入イベントの簡単な説明。侵入イベントをトリガーしたルール、デコーダ、またはプリプロセッサにより決定されます。
イベント メッセージ（Event Message）	dns response、P2P	イベントによって生成されるメッセージ。イベントをトリガーしたルール、デコーダ、またはプリプロセッサにより決定されます。
ファイル性質（File Disposition）	Malware、Clean	防御センターによるマルウェア クラウド ルックアップの実行対象ファイルの性質。この性質は、クラウドにより決定されます。
[ファイル名（File Name）]	Packages.bz2	ネットワーク トラフィックで検出されたファイルの名前
ファイル SHA256（File SHA256）	任意の 32 ビット文字列	防御センターによるマルウェア クラウド ルックアップの実行対象ファイルの SHA-256 ハッシュ値
ファイル タイプ（File Type）	GZ、SWF、MOV	ネットワーク トラフィックで検出されたファイルのタイプ

表 56-2　フィルタ データ タイプ(続き)

タイプ(Type)	値の例	定義(Definition)
ファイル タイプ カテゴリ(File Type Category)	`Archive、Multimedia、Executables`	ネットワーク トラフィックで検出されたファイルのタイプの一般カテゴリ
[IP アドレス(IP Address)]	`192.168.1.3、2001:0db8:85a3::0000/24`	IPv4 または IPv6 のアドレス、アドレス範囲、またはアドレス ブロック。 IP アドレスを検索すると、そのアドレスが送信元または宛先のいずれかになっているイベントが返されることに注意してください。
影響レベル(Impact Level)	`Impact Level 1、Impact Level 2`	モニタ対象ネットワークでのイベントの推定影響レベル
インライン結果(Inline Result)	`dropped、would have dropped`	トラフィックがドロップされたか、ドロップされた可能性があるか、またはシステムによりトラフィックが処理されていないかのいずれかです。
IOC カテゴリ	`High Impact Attack、Malware Detected`	トリガーとして使用された侵入の痕跡(IOC)イベントのカテゴリ
IOC イベント タイプ(IOC Event Type)	`exploit-kit、malware-backdoor`	特定の侵入の痕跡(IOC)に関連付けられている ID。その兆候をトリガーしたイベントを示します。
マルウェア脅威名(Malware Threat Name)	`W32.Trojan.a6b1`	マルウェア脅威の名前
[OS 名(OS Name)]	`Windows、Linux`	オペレーティング システムの名前
[OS のバージョン(OS Version)]	`XP、2.6`	オペレーティング システムの特定のバージョン
[プライオリティ(Priority)]	`high、low`	イベントの推定緊急度
セキュリティ インテリジェンスのカテゴリ(Security Intelligence Category)	`Malware、Spam`	Security Intelligence により判別される危険なトラフィックのカテゴリ
セキュリティ ゾーン	`My Security Zone、Security Zone X`	トラフィックが分析されたインターフェイスのセット。インライン展開の場合は、トラフィックが通過するインターフェイスのセット。
SSL	`yes, no`	SSL 暗号化トラフィック または TLS 暗号化トラフィック
ユーザ(User)	`wsmith、mtwain`	モニタ対象ネットワーク上のホストにログインしたユーザの ID

[フィルタ(Filter)] フィールドには、イベント検索と同様に、* や ! などの特殊検索パラメータを入力できます。フィルタ パラメータの前に ! 記号を付けることで排他的なフィルタを作成できます。FireSIGHT システムで一般にサポートされている検索制約の詳細については、検索でのワイルドカードと記号の使用(60-5 ページ)を参照してください。

複数のフィルタがアクティブな場合、同じデータ タイプの値は OR 検索条件として扱われます。つまり、いずれか 1 つの値と一致するデータがすべて表示されます。異なるデータ タイプの値は AND 検索条件として扱われます。つまり、データは各フィルタ データ タイプの 1 つ以上の値と一致する必要があります。たとえば、`Application: 2channel`、`Application: Reddit`、および `User: edickinson` というフィルタ セットで表示されるデータは、ユーザ `edickinson` に関連付けられており、**かつ**アプリケーション `2channel` **または**アプリケーション `Reddit` に関連付けられている必要があります。

フィルタのデータ タイプと値を確認した後で、新しいフィルタのデータ タイプと値を示すフィルタ ウィジェットがページの左上に表示されます。

複数のフィルタを設定してから適用したい場合もあるため、また Context Explorer ではすべてのセクションが完全にリロードされるまでに時間がかかることがあるため、追加したフィルタは自動的には適用されません。フィルタを適用するには、[フィルタの適用（Apply Filters）] をクリックする必要があります。設定されたがまだ適用されていないフィルタはぼかし表示されます。一度に最大 20 個のフィルタを適用できます。また、フィルタのウィジェットで削除アイコン（ ✖ ）をクリックして、個々のフィルタを削除することもできます。すべてのフィルタを一括削除するには、[削除（Clear）] ボタンをクリックします。

ファイル タイプの中には、相互に互換性がないタイプがあることに注意してください。たとえば、侵入イベント関連のフィルタ（**Device** や **Inline Result** など）を、接続イベント関連フィルタ（**Access Control Action** など）と同時に適用することはできません。これは、システムでは接続イベント データを侵入イベント データによってソートできないためです。互換性のないフィルタの同時適用はシステムによって自動的に防止されます。互換性の問題が存在する場合、より後に適用されたほうのフィルタ タイプと互換性のないタイプのフィルタは非表示になります。

表示されるデータは、管理対象デバイスのライセンスと導入方法、データを提供する機能を設定するかどうか、およびシリーズ 2アプライアンスの場合はデータを提供する機能をサポートしているかどうかなどの要因に応じて異なることに注意してください。たとえば DC500 防御センターとシリーズ 2デバイスはいずれも、カテゴリまたはレピュテーションによる URL フィルタリングをサポートしていないため、DC500 防御センターではこの機能のデータは表示されず、シリーズ 2デバイスではこのデータが検出されません。

[フィルタの追加（Add Filter）] ウィンドウで新しいフィルタを作成するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [Context Explorer] を選択します。

Context Explorer が表示されます。

手順 2　右上にある [フィルタ（Filter）] の下で、プラス アイコン（ ✚ ）をクリックします。

[フィルタの追加（Add Filter）] ポップアップ ウィンドウが表示されます。

手順 3　[データ タイプ（Data Type）] ドロップダウンリストから、フィルタリングの条件として使用するデータ タイプを選択します。

[フィルタ（Filter）] フィールドに、そのデータ タイプの値の例が取り込まれます。

手順 4　[フィルタ（Filter）] フィールドに、フィルタリングの条件として使用するデータ タイプ値を入力します。

手順 5　[OK] をクリックします。

フィルタが追加されます。Context Explorer が再び表示され、対応するフィルタ ウィジェットが表示されます。

手順 6　オプションで、前述の手順を繰り返し、必要なフィルタ セットが設定されるまで、フィルタを追加します。Context Explorer は自動的に更新されないため、フィルタを追加してもフィルタは適用されないことに注意してください。

手順 7　[フィルタの適用（Apply Filters）] をクリックします。

フィルタが適用され、Context Explorer が更新され、フィルタリングされたデータが反映されます。

フィルタを削除する方法：

アクセス：Admin/Any Security Analyst

手順 1　任意のフィルタ ウィジェットの削除アイコン（ ✖ ）をクリックします。

フィルタが削除されます。

すべてのフィルタをクリアする方法：

アクセス：Admin/Any Security Analyst

手順 1　フィルタ ウィジェットの右に表示される [クリア（Clear）] ボタンをクリックします。

すべてのフィルタがクリアされます。

フィルタが作成されていない場合、このボタンが表示されないことに注意してください。

コンテキスト メニューを使用したフィルタの作成

ライセンス：FireSIGHT

Context Explorer のグラフとリスト データを詳しく調べるときに、データ ポイントをクリックし、コンテキスト メニューを使用してそのデータに基づいてフィルタ（包含または除外）を簡単に作成できます。コンテキスト メニューを使用して、Application、User、または Intrusion Event Message データ タイプの情報、あるいは任意の個別ホストでフィルタリングする場合、フィルタ ウィジェットには、そのデータ タイプの該当する詳細ページ（アプリケーション データの場合は [アプリケーション詳細（Application Detail）] など）にリンクするウィジェット情報アイコンが表示されます。URL データではフィルタリングできないことに注意してください。

特定のグラフまたはリストのデータを詳しく調査する場合にもコンテキスト メニューを使用できます。詳細については、Context Explorer データのドリルダウン（56-41 ページ）を参照してください。

コンテキスト メニューからフィルタを作成する方法：

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [Context Explorer] を選択します。

Context Explorer が表示されます。

手順 2　[経時トラフィックおよび侵入イベント（Traffic and Intrusion Events over Time）] セクションと URL データを含むセクション以外の Explorer セクションで、フィルタリングするデータ ポイントをクリックします。

コンテキスト メニュー ポップアップ ウィンドウが表示されます。

手順 3　以下の 2 つの対処法があります。

- このデータにフィルタを追加するには、[フィルタの追加（Add Filter）] をクリックします。

  フィルタが追加され、そのウィジェットが左上に表示されます。
- このデータに除外フィルタを追加するには、[除外フィルタの追加（Add Exclude Filter）] をクリックします。このフィルタが適用されると、除外された値に関連付けられて**いない**すべてのデータが表示されます。

  フィルタが追加され、そのウィジェットが左上に表示されます。除外フィルタでは、フィルタ値の前に感嘆符が表示されます。

フィルタの詳細を表示する方法:

アクセス: Admin/Any Security Analyst

手順 1　該当するフィルタ ウィジェットの情報アイコン（  ）をクリックします。

新しいウィンドウが開き、フィルタのデータ タイプに関連する詳細ページが表示されます。

フィルタのブックマーク

ライセンス: FireSIGHT

フィルタは、必要とする正確な FireSIGHT データ コンテキストをいつでも取得できるシンプルかつ俊敏性に優れたツールとして機能します。永続的に設定するものではなく、Context Explorer から外部に移動するか、セッションを終了すると、消去されます。ただし、組織では特定のフィルタの組み合わせを頻繁に使用することがあります。フィルタ設定を後で使用できるように維持するには、そのフィルタを適用した Context Explorer のブラウザ ブックマークを作成できます。適用されるフィルタは Context Explorer ページ URL に組み込まれているので、そのページのブックマークを読み込むと、対応するフィルタも読み込まれます。