Context Explorer の使用法

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、侵害の兆候、侵入イベント、ホスト、サーバ、Security Intelligence、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、Administrator、Security Analyst、または Security Analyst (Read Only) 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くカスタマイズ可能であり、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% であるが、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 の防御センターと シリーズ 2 デバイスはいずれも拡張マルウェア検出をサポートしていないため、DC500 の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 4-1　比較：ダッシュボードおよび Context Explorer

機能	ダッシュボード	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、侵害の兆候、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、Security Intelligence 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
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」（P.3-1）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、侵害の兆候、ネットワーク、アプリケーション、Security Intelligence、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 でのフィルタ操作」（P.4-38）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。

- 「[Traffic and Intrusion Event Counts] グラフについて」（P.4-3）
- 「[Indications of Compromise] セクションについて」（P.4-4）
- 「[Network Information] セクションについて」（P.4-6）

- 「[Application Information] セクションについて」（P.4-10）
- 「[Security Intelligence] セクションについて」（P.4-15）
- 「[Intrusion Information] セクションについて」（P.4-17）
- 「[Files Information] セクションについて」（P.4-22）
- 「[Geolocation Information] セクションについて」（P.4-28）
- 「[URL Information] セクションについて」（P.4-31）

Context Explorer の全体的な設定方法については、次のトピックを参照してください。

- 「Context Explorer の更新」（P.4-35）
- 「Context Explorer の時間範囲の設定」（P.4-35）
- 「Context Explorer のセクションの最小化および最大化」（P.4-36）
- 「Context Explorer データのドリルダウン」（P.4-36）

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

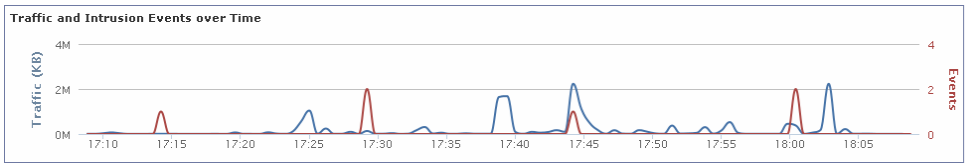
- 「Context Explorer でのフィルタ操作」（P.4-38）
- 「フィルタの追加および適用」（P.4-38）
- 「コンテキスト メニューを使用したフィルタの作成」（P.4-42）
- 「フィルタのブックマーク」（P.4-43）

[Traffic and Intrusion Event Counts] 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。

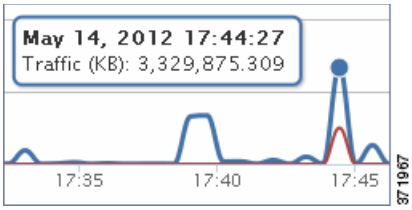
X 軸の最小間隔が 5 分であることに注意してください。これに対応するため、選択された時間範囲の開始点と終了点が、システムにより、最も近い 5 分間間隔に調整されます。



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だけがグラフに表示されます。たとえば、[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（[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 [Intrusion Events] 表と [Connection Events] 表のデータです。

[Indications of Compromise] セクションについて

ライセンス：FireSIGHT

Context Explorer の [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。

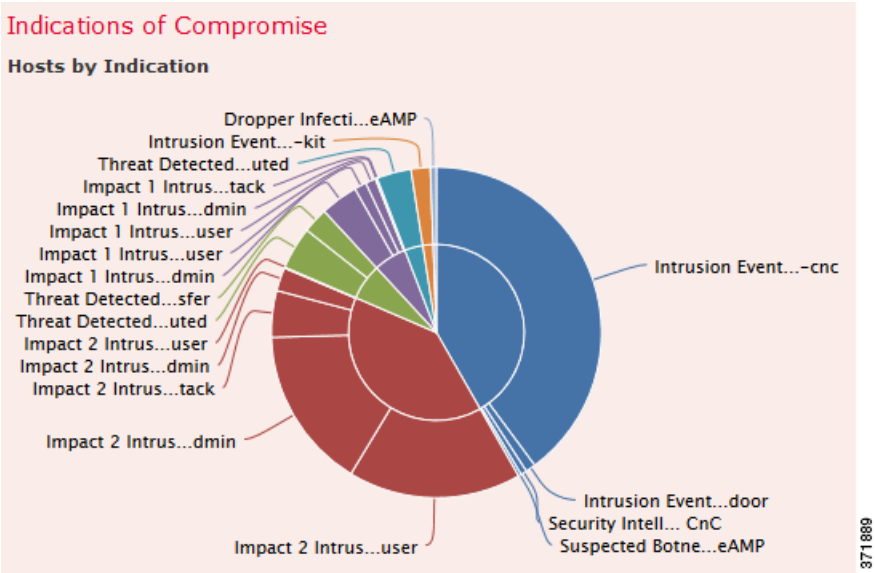
[Indications of Compromise] セクションのグラフの詳細については、次のトピックを参照してください。

- 「[Hosts by Indication] グラフの表示」（P.4-4）
- 「[Indications by Host] グラフの表示」（P.4-5）

[Hosts by Indication] グラフの表示

ライセンス：FireSIGHT

[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害の兆候（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。



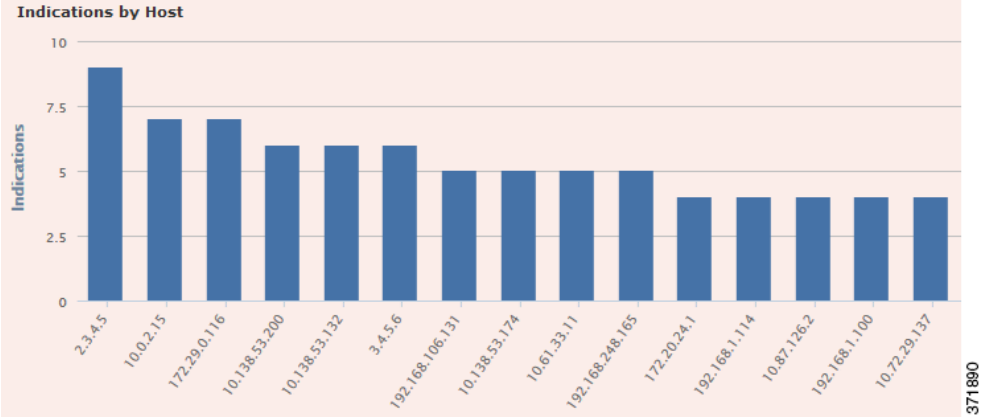
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [Hosts] 表と [Indications of Compromise] 表から取得されます。

[Indications by Host] グラフの表示

ライセンス：FireSIGHT

[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害の兆候（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 [Hosts] 表と [Indications of Compromise] 表から取得されます。

[Network Information] セクションについて

ライセンス：FireSIGHT

Context Explorer の [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。

[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。

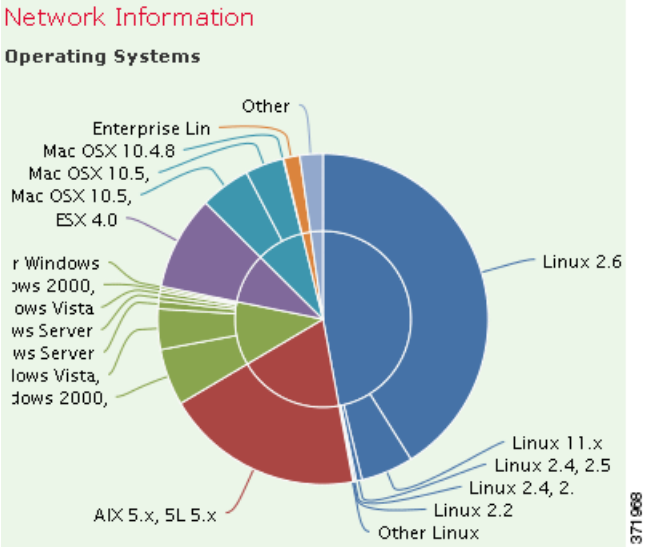
- 「[Operating Systems] グラフの表示」（P.4-6）
- 「[Traffic by Source IP] グラフの表示」（P.4-7）
- 「[Traffic by Source User] グラフの表示」（P.4-7）
- 「[Connections by Access Control Action] グラフの表示」（P.4-8）
- 「[Traffic by Destination IP] グラフの表示」（P.4-9）
- 「[Traffic by Ingress/Egress Security Zone] グラフの表示」（P.4-9）

[Operating Systems] グラフの表示

ライセンス：FireSIGHT

[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 [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。



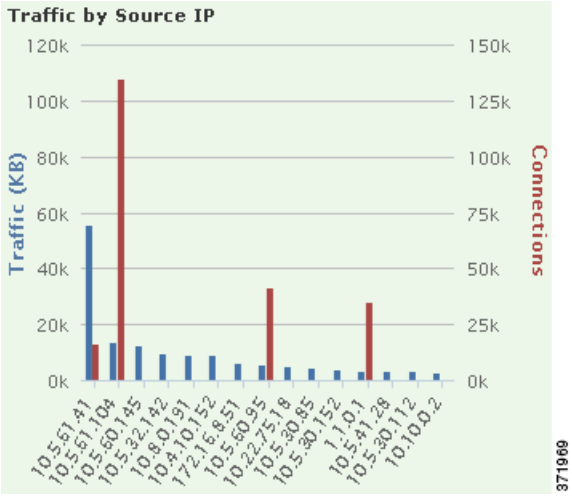
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [Hosts] 表から取得されます。

[Traffic by Source IP] グラフの表示

ライセンス：FireSIGHT

[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。

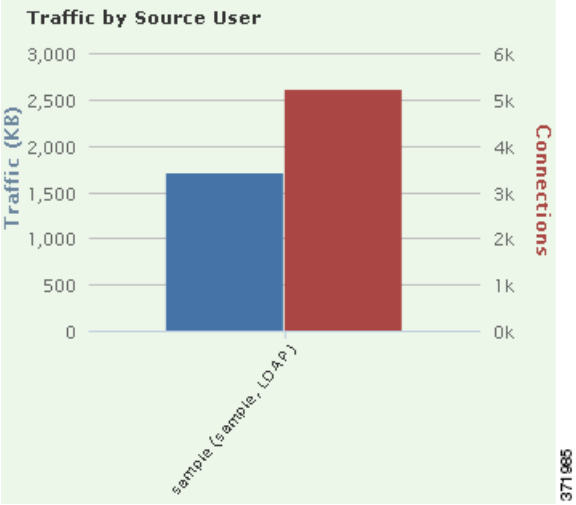
注　侵入イベントの情報でフィルタリングすると、[Traffic by Source IP] グラフは非表示になります。

このグラフのデータは主に [Connection Events] 表から取得されます。

[Traffic by Source User] グラフの表示

ライセンス：FireSIGHT

[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。

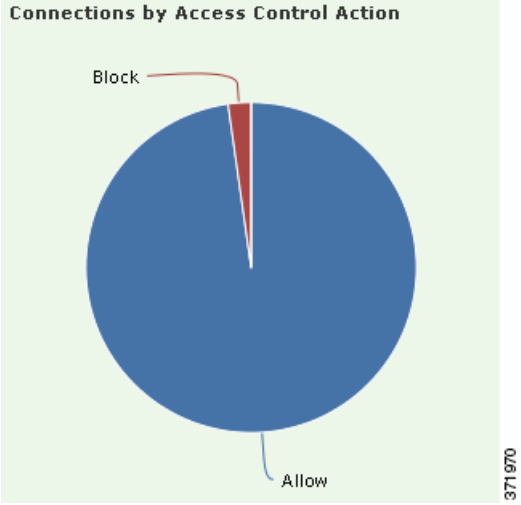
注　侵入イベントの情報でフィルタリングすると、[Traffic by Source User] グラフは非表示になります。

このグラフのデータは主に [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だけが表示されることに注意してください。

[Connections by Access Control Action] グラフの表示

ライセンス：FireSIGHT

[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（[Block] や [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。

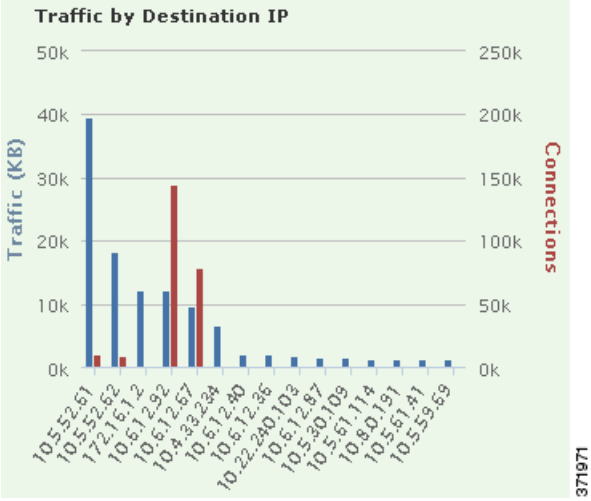
注　侵入イベントの情報でフィルタリングすると、[Traffic by Source User] グラフは非表示になります。

このグラフのデータは主に [Connection Events] 表から取得されます。

[Traffic by Destination IP] グラフの表示

ライセンス：FireSIGHT

[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、[Traffic by Destination IP] グラフは非表示になります。

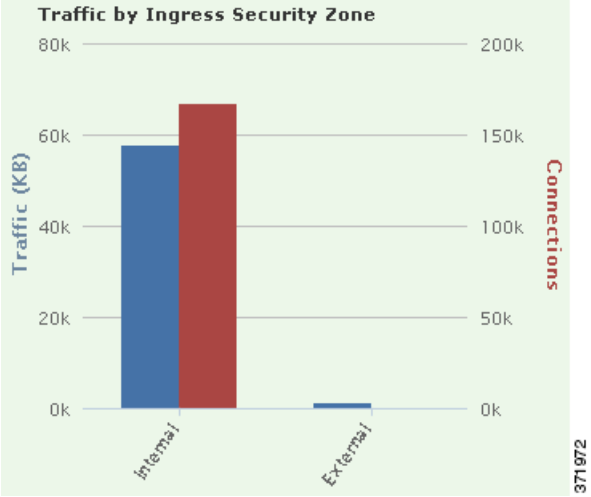
このグラフのデータは主に [Connection Events] 表から取得されます。

[Traffic by Ingress/Egress Security Zone] グラフの表示

ライセンス：FireSIGHT

[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」（P.5-43）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 [Egress] をクリックします。デフォルト ビューに戻すには [Ingress] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [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、[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 [Connection Events] 表から取得されます。

[Application Information] セクションについて

ライセンス：FireSIGHT

Context Explorer の [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リスクまたは推定ビジネス関連度ごとに編成したもの）を示します。[Application Details List] は、各アプリケーションとそのリスク、ビジネス関連度、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、[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 [Application Information] セクションを設定することもできます。

[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。

- 「[Traffic by Risk/Business Relevance and Application] グラフの表示」（P.4-11）
- 「[Intrusion Events by Risk/Business Relevance and Application] グラフの表示」（P.4-12）
- 「[Hosts by Risk/Business Relevance and Application] グラフの表示」（P.4-13）
- 「[Application Details List] の表示」（P.4-14）

[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

ステップ 1　[Analysis] > [Context Explorer] を選択します。

Context Explorer が表示されます。

ステップ 2　[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[Client Application Information] または [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。

ステップ 3　[Application Protocol]、[Client Application]、または [Web Application] をクリックします。

[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。

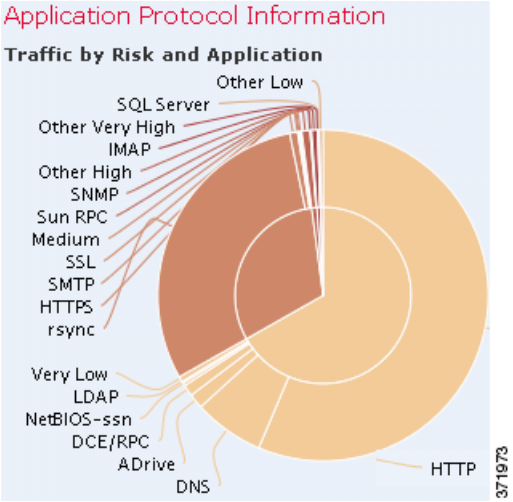
注　Context Explorer の外部に移動すると、このセクションはデフォルトの状態（Application Protocol）に戻ります。

[Traffic by Risk/Business Relevance and Application] グラフの表示

ライセンス：FireSIGHT

[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リスク（デフォルト）または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル（`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 [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、ビジネス関連度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 [Risk] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Risk] ビューに戻ることに注意してください。

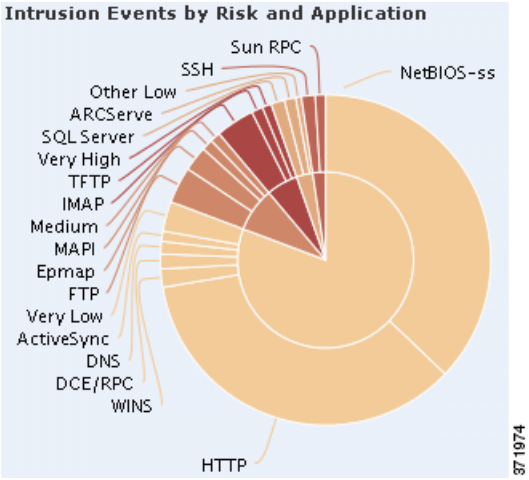
注　侵入イベントの情報でフィルタリングすると、[Traffic by Risk/Business and Application] グラフは非表示になります。

このグラフのデータは主に [Connection Events] 表と [Application Statistics] 表から取得されます。

[Intrusion Events by Risk/Business Relevance and Application] グラフの表示

ライセンス：FireSIGHT

[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リスク（デフォルト）または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル（`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 [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。

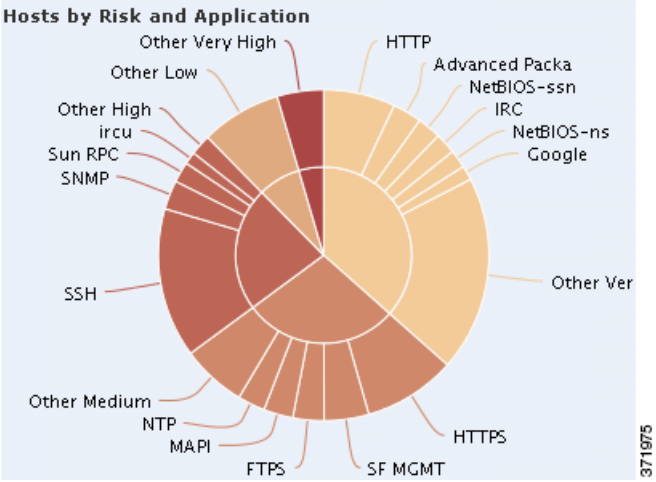
ヒント　グラフに制約を適用して、ビジネス関連度とアプリケーションごとに侵入イベントが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Business Relevance] をクリックします。デフォルト ビューに戻すには [Risk] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Risk] ビューに戻ることに注意してください。

このグラフのデータは主に [Intrusion Events] 表と [Application Statistics] 表から取得されます。

[Hosts by Risk/Business Relevance and Application] グラフの表示

ライセンス：FireSIGHT

[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リスク（デフォルト）または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル（`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 [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、ビジネス関連度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 [Business Relevance] をクリックします。デフォルト ビューに戻すには [Risk] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [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 [Applications] 表から取得されます。

[Application Details List] の表示

ライセンス：FireSIGHT

[Application Information] セクション下部に表示される [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リスク、推定ビジネス関連度、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。

[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 [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。

[Security Intelligence] セクションについて

ライセンス：Protection

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

サポート対象防御センター：DC500 を除くすべて

Context Explorer の [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 Security Intelligence 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、カテゴリ、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。

[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。

- 「[Security Intelligence Traffic by Category] グラフの表示」（P.4-15）
- 「[Security Intelligence Traffic by Source IP] グラフの表示」（P.4-16）
- 「[Security Intelligence Traffic by Destination IP] グラフの表示」（P.4-17）

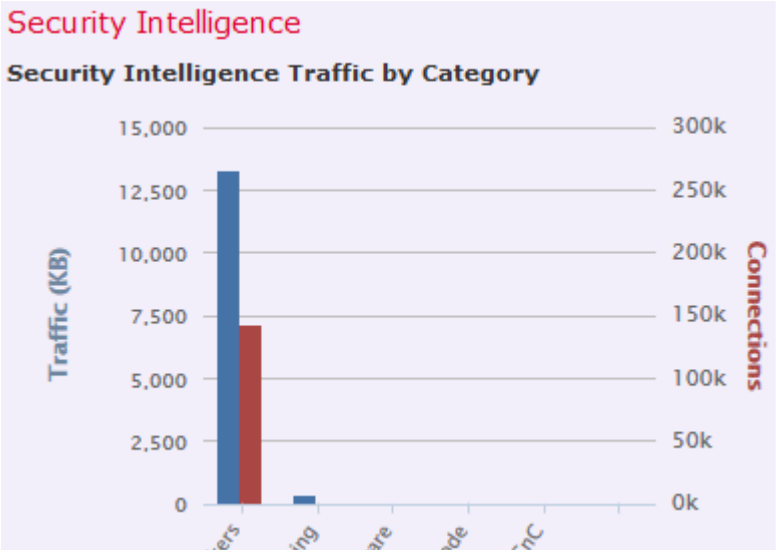
[Security Intelligence Traffic by Category] グラフの表示

ライセンス：Protection

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

サポート対象防御センター：DC500 を除くすべて

[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 Security Intelligence 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、[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 [Security Intelligence] 表から取得されます。

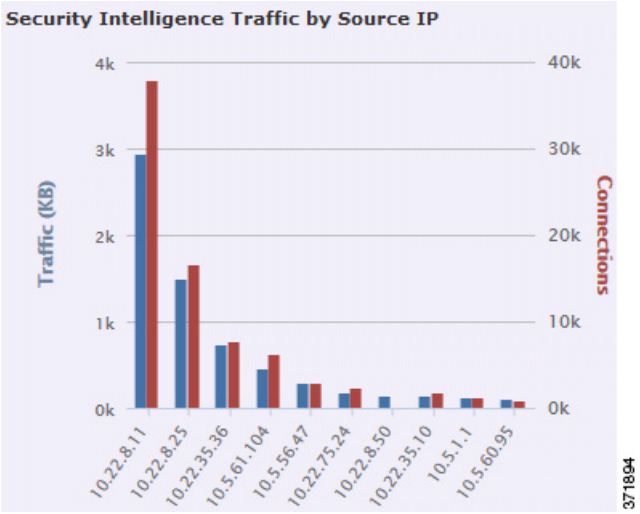
[Security Intelligence Traffic by Source IP] グラフの表示

ライセンス：Protection

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

サポート対象防御センター：DC500 を除くすべて

[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 Security Intelligence 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、[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 [Security Intelligence] 表から取得されます。

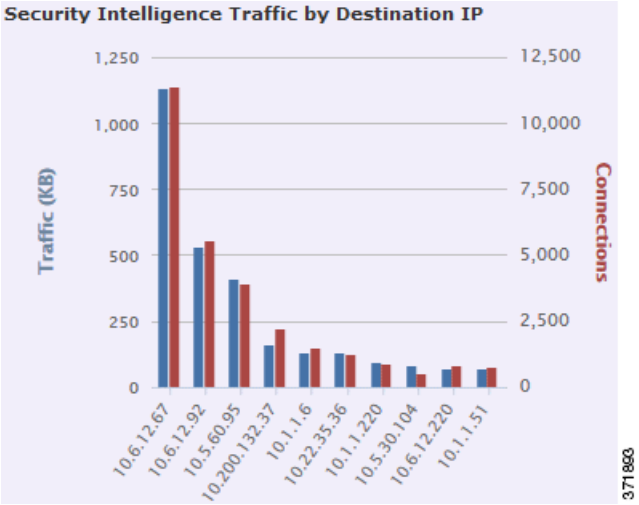
[Security Intelligence Traffic by Destination IP] グラフの表示

ライセンス：Protection

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

サポート対象防御センター：DC500 を除くすべて

[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 Security Intelligence によってモニタされるトラフィックの上位の宛先 IP アドレスごとに、そのネットワーク 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、[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 [Security Intelligence] 表から取得されます。

[Intrusion Information] セクションについて

ライセンス：Protection

Context Explorer の [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。

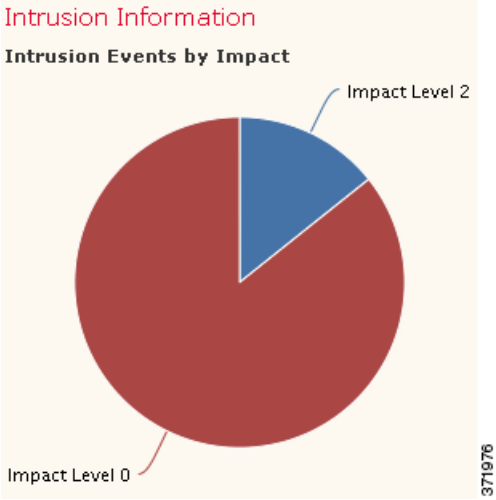
[Network Information] セクションのグラフとリストの詳細については、次のトピックを参照してください。

- 「[Intrusion Events by Impact] グラフの表示」（P.4-18）
- 「[Top Attackers] グラフの表示」（P.4-18）
- 「[Top Users] グラフの表示」（P.4-19）
- 「[Intrusion Events by Priority] グラフの表示」（P.4-20）
- 「[Top Targets] グラフの表示」（P.4-20）
- 「[Top Ingress/Egress Security Zones] グラフの表示」（P.4-21）
- 「[Intrusion Event Details List] の表示」（P.4-21）

[Intrusion Events by Impact] グラフの表示

ライセンス：Protection

[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。



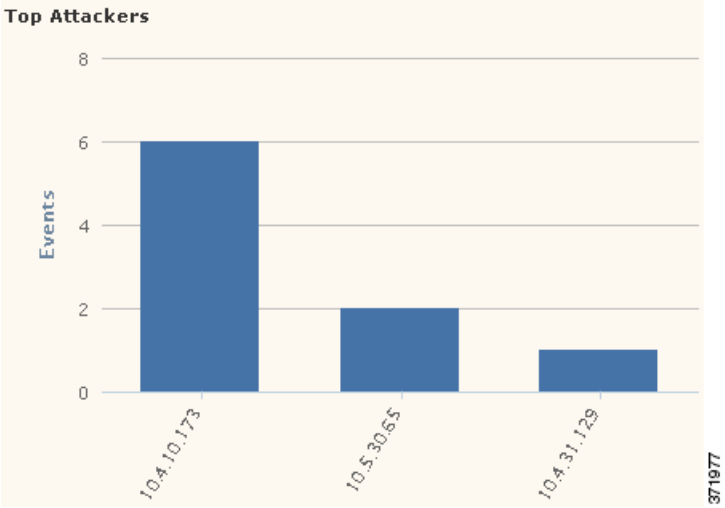
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [Intrusion Events] 表と [IDS Statistics] 表から取得されます。

[Top Attackers] グラフの表示

ライセンス：Protection

[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。



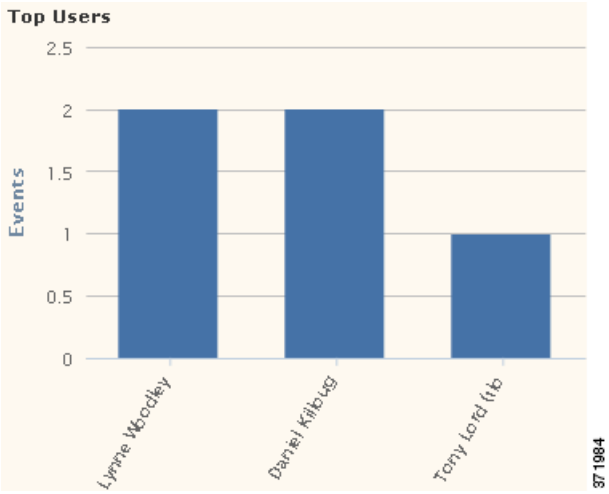
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [Intrusion Events] 表から取得されます。

[Top Users] グラフの表示

ライセンス：Protection

[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。



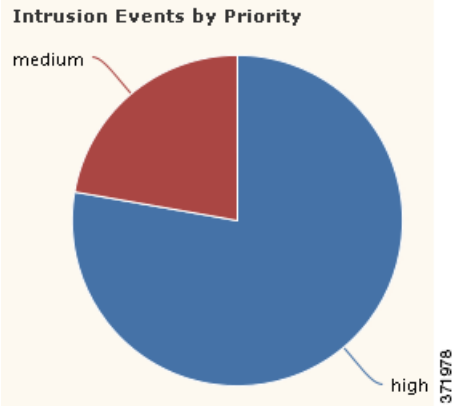
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [Intrusion Events] 表と [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だけが表示されることに注意してください。

[Intrusion Events by Priority] グラフの表示

ライセンス：Protection

[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。



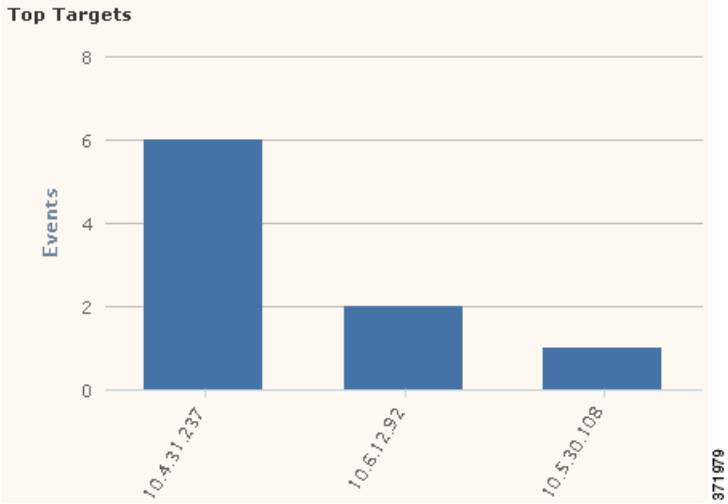
グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [Intrusion Events] 表から取得されます。

[Top Targets] グラフの表示

ライセンス：Protection

[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 [Intrusion Events] 表から取得されます。

[Top Ingress/Egress Security Zones] グラフの表示

ライセンス：Protection

[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」（P.5-43）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 [Egress] をクリックします。デフォルト ビューに戻すには [Ingress] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [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 [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。

[Intrusion Event Details List] の表示

ライセンス：Protection

[Intrusion Information] セクション下部に表示される [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。

[Event 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することができます。この表のデータは主に [Intrusion Events] 表から取得されます。

[Files Information] セクションについて

ライセンス：Protection または Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

Context Explorer の [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、[File Information] セクション全体が非表示になります。

[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 の防御センターと シリーズ 2 デバイスはいずれも拡張マルウェア検出をサポートしていないため、DC500 の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。「マルウェア対策とファイル制御について」（P.33-3）を参照してください。

[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。

- 「[Top File Types] グラフの表示」（P.4-22）
- 「[Top File Names] グラフの表示」（P.4-23）
- 「[Files by Disposition] グラフの表示」（P.4-24）
- 「[Top Hosts Sending Files] グラフ」（P.4-25）
- 「[Top Hosts Receiving Files] グラフ」（P.4-26）
- 「[Top Malware Detections] グラフの表示」（P.4-27）

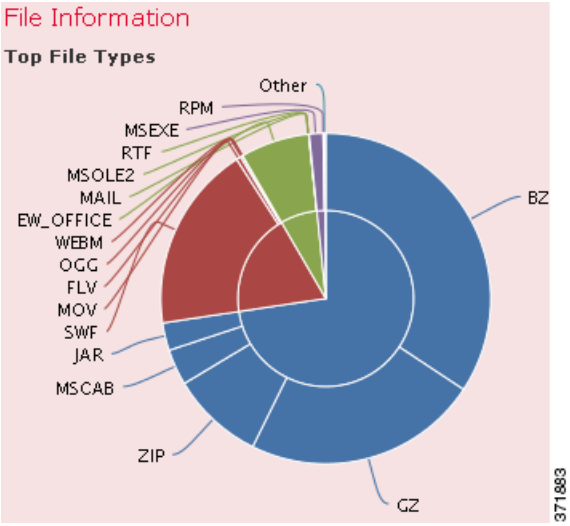
[Top File Types] グラフの表示

ライセンス：Protection または Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

[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 の防御センターと シリーズ 2 デバイスはいずれも拡張マルウェア検出をサポートしていないため、DC500 の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。「マルウェア対策とファイル制御について」（P.33-3）を参照してください。

このグラフのデータは主に [File Events] 表から取得されます。

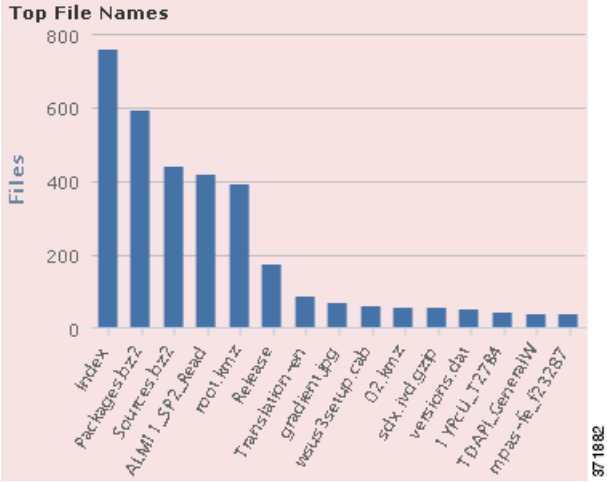
[Top File Names] グラフの表示

ライセンス：Protection または Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

[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 の防御センターと シリーズ 2 デバイスはいずれも拡張マルウェア検出をサポートしていないため、DC500 の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。「マルウェア対策とファイル制御について」（P.33-3）を参照してください。

このグラフのデータは主に [File Events] 表から取得されます。

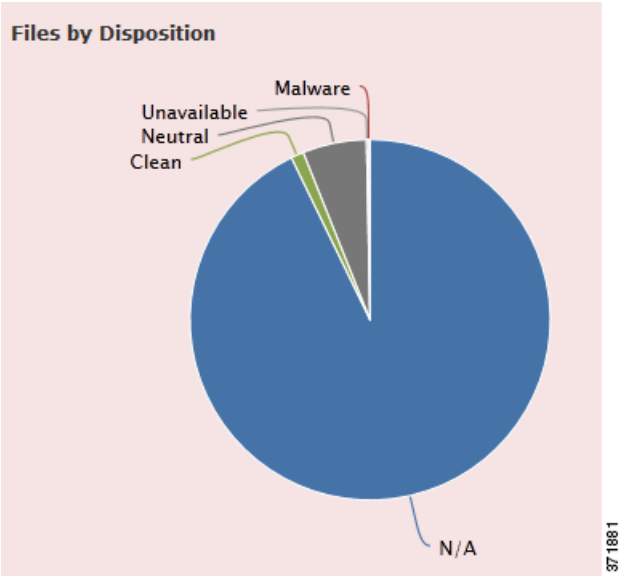
[Files by Disposition] グラフの表示

ライセンス：Protection または Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

[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 検索（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。クラウド検索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 クラウド検索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「マルウェア対策とファイル制御について」（P.33-3）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 の防御センターと シリーズ 2 デバイスはいずれも拡張マルウェア検出をサポートしていないため、DC500 の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。「マルウェア対策とファイル制御について」（P.33-3）を参照してください。

このグラフのデータは主に [File Events] 表から取得されます。

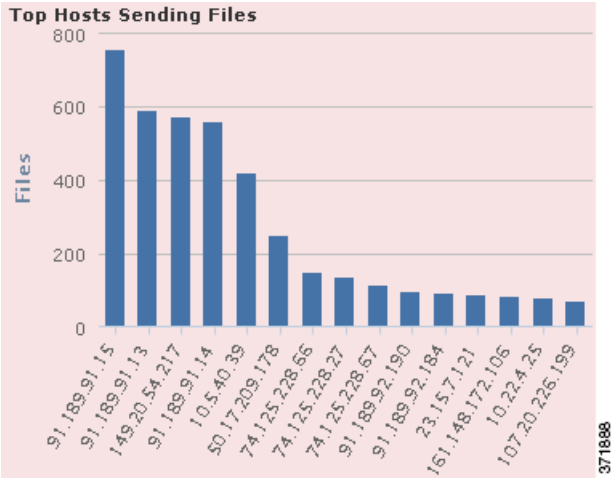
[Top Hosts Sending Files] グラフ

ライセンス：Protection または Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

[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 [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 [Files] をクリックします。Context Explorer から外部へ移動することでも、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 の防御センターと シリーズ 2 デバイスはいずれも拡張マルウェア検出をサポートしていないため、DC500 の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。「マルウェア対策とファイル制御について」（P.33-3）を参照してください。

このグラフのデータは主に [File Events] 表から取得されます。

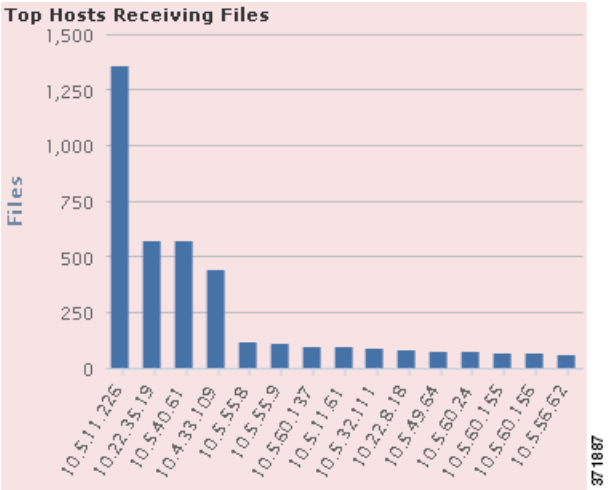
[Top Hosts Receiving Files] グラフ

ライセンス：Protection または Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

[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 [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 [Files] をクリックします。Context Explorer から外部へ移動することでも、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 の防御センターと シリーズ 2デバイスはいずれも拡張マルウェア検出をサポートしていないため、DC500 の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。「マルウェア対策とファイル制御について」（P.33-3）を参照してください。

このグラフのデータは主に [File Events] 表から取得されます。

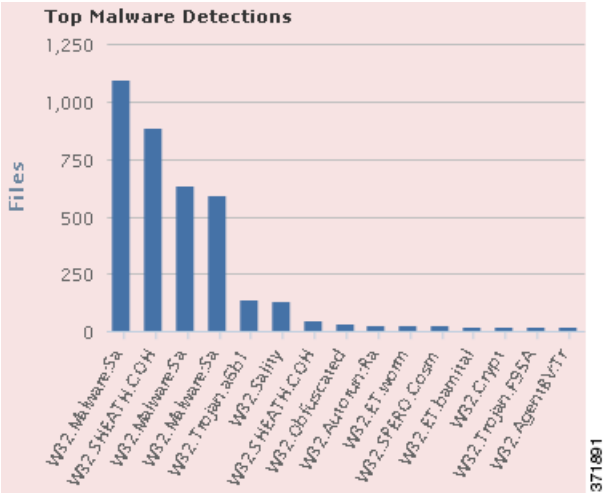
[Top Malware Detections] グラフの表示

ライセンス：Protection または Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

[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 の防御センターと シリーズ 2 デバイスはいずれも拡張マルウェア検出をサポートしていないため、DC500 の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。「マルウェア対策とファイル制御について」（P.33-3）を参照してください。

このグラフのデータは主に [File Events] 表と [Malware Events] 表から取得されます。

[Geolocation Information] セクションについて

ライセンス：FireSIGHT

サポート対象防御センター：DC500 を除くすべて

Context Explorer の [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。

[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。

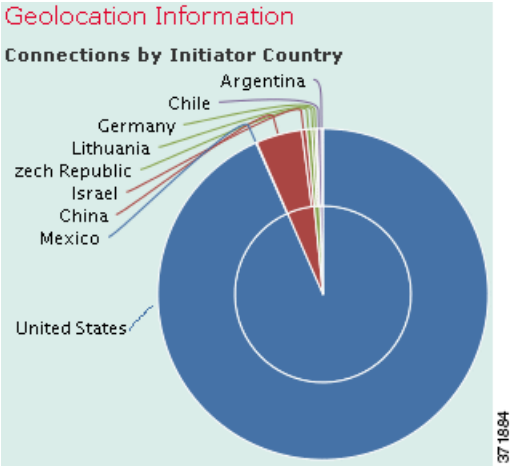
- 「[Connections by Initiator/Responder Country] グラフの表示」（P.4-29）
- 「[Intrusion Events by Source/Destination Country] グラフの表示」（P.4-29）
- 「[File Events by Sending/Receiving Country] グラフの表示」（P.4-30）

[Connections by Initiator/Responder Country] グラフの表示

ライセンス：FireSIGHT

サポート対象防御センター：DC500 を除くすべて

[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、「地理情報の使用」（P.47-24）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」（P.16-1）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 [Responder] をクリックします。デフォルト ビューに戻すには [Initiator] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの[Initiator] ビューに戻ることに注意してください。

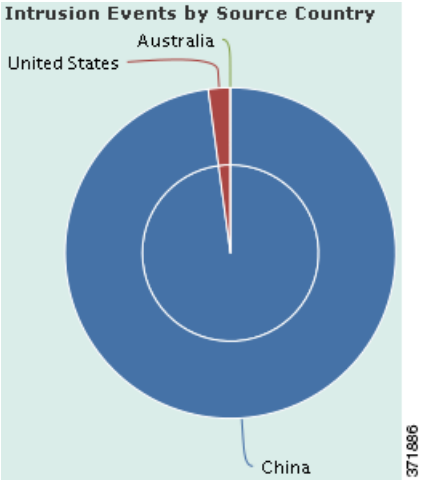
このグラフのデータは主に [Connection Summary Data] 表から取得されます。

[Intrusion Events by Source/Destination Country] グラフの表示

ライセンス：FireSIGHT

サポート対象防御センター：DC500 を除くすべて

[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、「地理情報の使用」（P.47-24）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」（P.18-1）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 [Destination] をクリックします。デフォルト ビューに戻すには [Source] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Source] ビューに戻ることに注意してください。

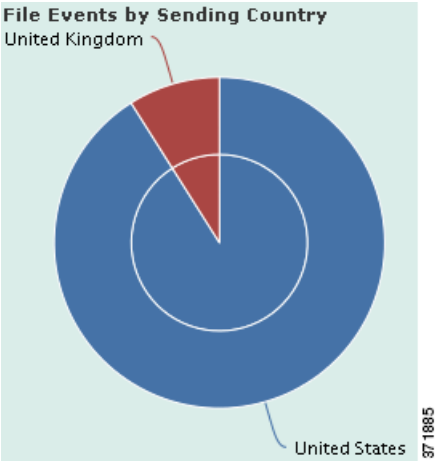
このグラフのデータは主に [Intrusion Events] 表から取得されます。

[File Events by Sending/Receiving Country] グラフの表示

ライセンス：FireSIGHT

サポート対象防御センター：DC500 を除くすべて

[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、「地理情報の使用」（P.47-24）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」（P.34-8）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 [Receiver] をクリックします。デフォルト ビューに戻すには [Sender] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [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 [File Events] 表から取得されます。

[URL Information] セクションについて

ライセンス：FireSIGHT または URL Filtering

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

Context Explorer の [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 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 Filtering ライセンスを所有しており、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の防御センターと 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の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 条件の追加」（P.14-31）を参照してください。

[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。

- 「[Traffic by URL] グラフの表示」（P.4-32）
- 「[Traffic by URL Category] グラフの表示」（P.4-33）
- 「[Traffic by URL Reputation] グラフの表示」（P.4-34）

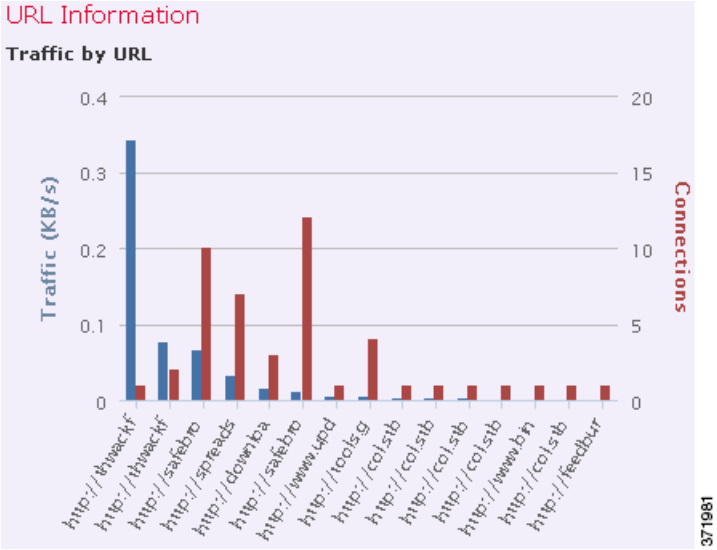
[Traffic by URL] グラフの表示

ライセンス：FireSIGHT または URL Filtering

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

[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、[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 Filtering ライセンスを所有しており、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の防御センターと 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の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」（P.51-27）を参照してください。

このグラフのデータは主に [Connection Events] 表から取得されます。

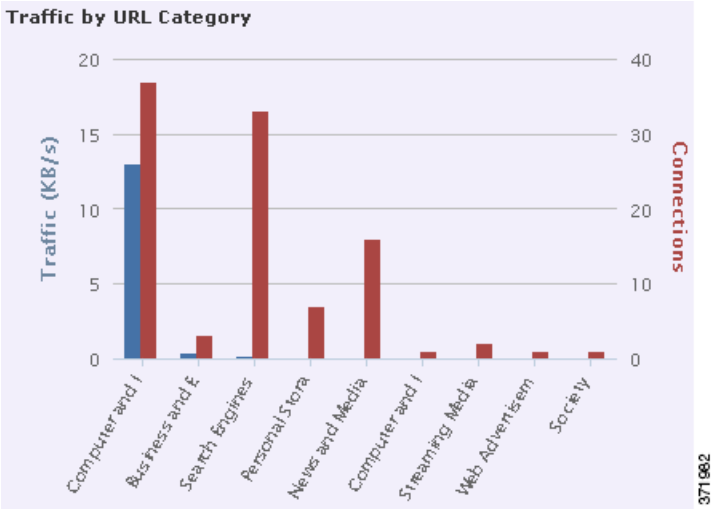
[Traffic by URL Category] グラフの表示

ライセンス：URL Filtering

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

[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、[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 Filtering ライセンスを所有しており、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の防御センターと 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の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 条件の追加」（P.14-31）を参照してください。

このグラフのデータは主に [URL Statistics] 表と [Connection Events] 表から取得されます。

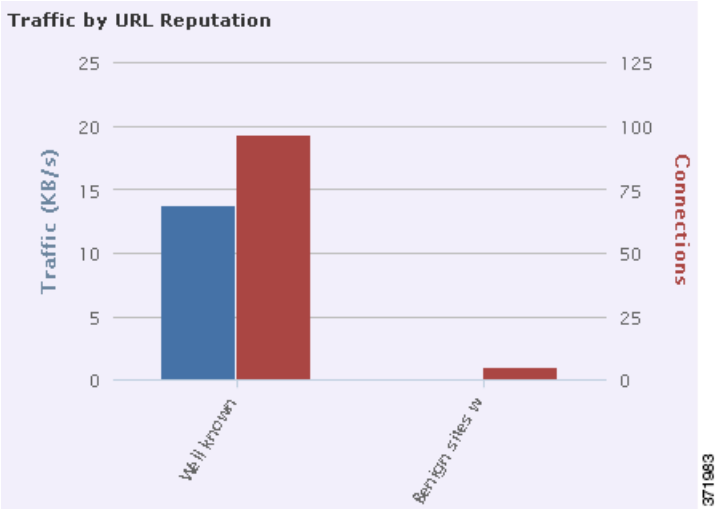
[Traffic by URL Reputation] グラフの表示

ライセンス：URL Filtering

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

[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、[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 Filtering ライセンスを所有しており、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の防御センターと 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の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 条件の追加」（P.14-31）を参照してください。

このグラフのデータは主に [URL Statistics] 表と [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。

（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により）Context Explorer 自体をリロードすると、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 [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

ステップ 1　Context Explorer の右上にある [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 [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 は変更を反映するために自動的に更新され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

ステップ 1　[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。

ステップ 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、[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　[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。[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

ステップ 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

ステップ 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。（[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、[Traffic by Source IP] グラフの IP アドレスでドリルダウンすると、[Connection Events] 表の [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 でのフィルタ操作」（P.4-38）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

ステップ 1　[Analysis] > [Context Explorer] を選択します。

Context Explorer が表示されます。

ステップ 2　[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。

ステップ 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、[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、[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」（P.37-1）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、[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」（P.35-12）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、[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」（P.38-65）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、[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」（P.21-6）を参照してください。

- 特定のファイル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、そのファイルのトラジェクトリを参照するには、[View Network File Trajectory] を選択します。

  新しいウィンドウが開き、選択したファイルのトラジェクトリ マップが表示されます。ネットワーク ファイル トラジェクトリ機能の使用の詳細については、「ネットワーク ファイル トラジェクトリの操作」（P.34-31）を参照してください。

- 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、[Blacklist Now] または [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 ウィンドウの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」（P.5-7）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より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」（P.4-38）
- 「コンテキスト メニューを使用したフィルタの作成」（P.4-42）
- 「フィルタのブックマーク」（P.4-43）

フィルタの追加および適用

ライセンス：FireSIGHT、Protection、Control、またはMalware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

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。

- [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（ sf ）または特定の詳細ビュー ページ（[Application Detail]、[Host Profile]、[Rule Detail]、[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、[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」（P.4-42）を参照してください。

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

[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 [Filter] フィールドに入力します（たとえば、[Continent] タイプの場合は値 `Asia` など）。ユーザ支援のため、[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 の防御センターでは、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 アプライアンス機能の要約については、「管理対象デバイスの各モデルでサポートされる機能」の表を参照してください。

表 4-2　フィルタ データ タイプ

タイプ	値の例	定義
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制御ポリシーにより実行されるアクション
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
Application Name	`Facebook`、`HTTP`	アプリケーションの名前
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
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）。
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）
Business Relevance	`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
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
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
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。
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。
File Disposition	`Malware`、`Clean`	防御センターによるマルウェア クラウド検索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。
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
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 クラウド検索の実行対象ファイルの SHA-256 ハッシュ値

表 4-2　フィルタ データ タイプ（続き）

タイプ	値の例	定義
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
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 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。
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
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 Category	High Impact Attack、Malware Detected	トリガーとして使用された侵害の兆候（IOC）イベントのカテゴリ
IOC Event Type	exploit-kit、malware-backdoor	特定の侵害の兆候（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。
Malware Threat Name	W32.Trojan.a6b1	マルウェア脅威の名前
OS Name	Windows、Linux	オペレーティング システム名
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
Priority	high、low	イベントの推定緊急度
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
Security Zone	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。
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

[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 ! 記号を入力することにより、除外フィルタを作成することができます。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」（P.45-4）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（AND）**アプリケーション 2channel **または（OR）**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、[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、[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 の防御センターと 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 の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。

[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

ステップ 1　[Analysis] > [Context Explorer] を選択します。

Context Explorer が表示されます。

ステップ 2　右上にある [Filter] の下で、プラス アイコン（ ＋ ）をクリックします。

[Add Filter] ポップアップ ウィンドウが表示されます。

ステップ 3　[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。

[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。

ステップ 4　[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。

ステップ 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。

ステップ 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。

ステップ 7　[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

ステップ 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

ステップ 1　フィルタ ウィジェットの右に表示される [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 [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」（P.4-36）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

ステップ 1　[Analysis] > [Context Explorer] を選択します。

Context Explorer が表示されます。

ステップ 2　[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。

ステップ 3　次の 2 つのオプションから選択できます。

- このデータにフィルタを追加するには、[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、[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

ステップ 1　該当するフィルタ ウィジェットの情報アイコン（ i ）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。